Ελλειπτικες Καμπυλες και Κρυπτογραφια

Γεωργαντάς Χρήστος

Πτυχιακη Εργασια
Τμημα Μαθηματικων
Πανεπιστημιου Αιγαιου

Επιβλέπων Κοντογεώργης Αριστείδης

Σάμος 2003

Στην αδερφή μου Βασιλική

« Τα μαθηματικά είναι η βασίλισσα των επιστημών» Karl.F.Gauss

Περιεχόμενα

Εισαγωγή

Για την παρουσίαση αυτής της εργασίας αντλήσαμε υλικό από το βιβλίο ελλειπτικών καμπύλων του Γιάννη Αντωνιάδη [1]. Για τη μέθοδο του Pollard και τη παραγοντοποίηση με χρήση ελλειπτικών καμπύλων το υπό συγγραφή βιβλίο του W.Stein [6], καθώς και το βιβλίο των Silverman-Tate [7].

Οι υπολογισμοί πάνω στις ελλειπτικές καμπύλες έγιναν με το gp-pari, ενώ οι γραφικές παραστάσεις με το maple v9 και με το kig.

Ο όρος «ελλειπτικές καμπύλες» οφείλεται στις προσπάθειες των μαθηματικών του 18 αιώνα να υπολογίσουν τα περίφημα ελλειπτικά ολοκληρώματα, τα οποία προέκυψαν από την ανάγκη μέτρησης τμήματος τόξων ελλείψεων. Μεγάλες μορφές της ανάλυσης όπως Weierstass Jacobi και ο Abel ασχολήθηκαν με αυτά και ανακάλυψαν την διπλή περιοδικότητα των ελλειπτικών συναρτήσεων η οποία είχε σαν αποτέλεσμα ότι το σύνολο των σημείων του $\mathbb{P}^2(\mathbb{C})$ που επαληθεύουν μια εξίσωση της μορφής

$$zy^2 = x^3 + axz^2 + bz^3$$

έχει τη δομή ομάδας. Ένα τέτοιο σύνολο μπορεί να αποδειχθεί ότι είναι ισομορφικό με τον τόρο $\mathbb{C}/L \cong S^1 \times S^1$, όπου το L είναι ένα rank 2 $\mathbb{Z}$ module στο $\mathbb{C}$

Ο Poincare έδωσε εναλλακτικό τρόπο ορισμού της πρόσθεσης σημείων πάνω στην ελλειπτική καμπύλη αποδεικνείοντας ότι συνευθειακά σημεία έχουν άθροισμα O. Το γεγονός αυτό οδήγησε σε ένα εντελώς αλγεβρικό ορισμό της δομής ομάδας της ελλειπτικής καμπύλης, ο οποίος έδωσε τη δυνατότητα να ορίσουμε δομή ομάδας πάνω στο σύνολο $E(k)$ του προβολικού επιπέδου $\mathbb{P}^2(k)$ που ικανοποιούν την εξίσωση

$$z^2y^2 = x^3 + axz^2 + bz^3,$$

όπου τώρα το k είναι ένα τυχαίο σώμα.

Οι εφαρμογές της θεωρίας των ελλειπτικών καμπύλων είναι πολλές και ενδιαφέρουσες, στην Θεωρία των Αριθμών και στις Διοφαντικές εξισώσεις. Στην εργασία αυτή θα ασχοληθούμε με εφαρμογές που σχετίζονται με την κρυπτογραφία. Θα δούμε πώς μπορούμε να παραγοντοποιήσουμε αριθμούς κάνοντας χρήση ελλειπτικών καμπύλων και πώς μπορούμε να ορίσουμε κρυπτοσυστήματα El-Gamal κάνοντας χρήση της ομάδας της ελλειπτικής καμπύλης $E(\mathbb{F}_p)$ που ορίζεται πάνω από ένα πεπερασμένο σώμα.

Πρώτα από όλα, πρέπει να ευχαριστήσω τον επιβλέποντα καθηγητή αυτής της εργασίας τον κύριο Κοντογεώργη Αριστείδη. Επίσης τους καθηγητές, κυρίους

Μεταφτσή Βασίλειο και Σταματίου Ιωάννη, για το χρόνο που διέθεσαν να διαβάσουν την εργασία, καθώς και για τις εύστοχες παρατηρήσεις τους. Το επόμενο πρόσωπο που νιώθω ότι πρέπει να ευχαριστήσω είναι η αδερφή μου Βασιλική, για την ψυχολογική στήριξη που μου παρείχε όλο αυτό τον καιρό. Ακόμα ευχαριστώ θερμά τους κυρίους καθηγητές Τσολομύτη Αντώνιο και Τσαπόγα Γεώργιο για τις συμβουλές τους σε σχέση με θέματα μεταπτυχιακών σπουδών. Τέλος ευχαριστώ τον φίλο Κοψίδη Αλέξαντρο και την ξαδέρφη μου Κουτσογιάννη Παναγιώτα που με βοήθησαν στη μετάφραση Αγγλικών κειμένων.

Κεφάλαιο 1

Στοιχεία Θεωρίας Ελλειπτικών Καμπύλων.

1.1 Στοιχεία θεωρίας σωμάτων

Ορισμός 1 *Αν* $(R,+,\cdot)$ *δακτύλιος και* $(R-\{0\},\cdot)$ *είναι πολλαπλασιαστική ομάδα τότε το* R *λέγεται σώμα.*

Ορισμός 2 *Το σύνολο των πολυωνύμων με συντελεστές σε ένα δακτύλιο* R *συμβολίζεται με* $R[x]$.

Ορισμός 3 *Έστω* R *δακτύλιος. Αν υπάρχουν ακέραιοι μη μηδενικοί έτσι ώστε* $na = 0\ \forall a \in R$ *τότε ο ελάχιστος θετικός από αυτούς τους ακέραιους λέγεται χαρακτηριστική του* R. *Αν τέτοιος ακέραιος δεν υπάρχει τότε λέμε ότι ο δακτύλιος έχει χαρακτηριστική μηδέν.*

Έστω K, L σώματα τέτοια ώστε $K \subset L$. Το L θα λέγεται επέκταση του K την οποία θα συμβολίζουμε με L/K.

Θεώρημα 1 *: Το* L *μπορούμε να το δούμε σαν διανυσματικό χώρο πάνω από το* K.

Απόδειξη: Έστω $a, b \in L$ και $\alpha, \beta \in K$ τότε:

- $a\alpha \in L$
- $a(ba) = (ab)a$
- $(a+b)\alpha = a\alpha + b\alpha$
- $a(\alpha+\beta) = a\alpha + a\beta$
- $1\alpha = \alpha$

Η διάσταση του L είναι ο βαθμός της επέκτασης L/K και θα την συμβολίζουμε με $[L:K] := \dim_K L$. Προφανώς αν $[L:K]=1$ τότε $L = K$. Ισχύει για τις επεκτάσεις L/K και M/L

$$[M:K] = [M:L][L:K]$$

Απόδειξη: Έστω $a_1, ..., a_m$ βάση του $[L:K]$ και $b_1, ..., b_m$ βάση του $[M:L]$. Τότε $\{a_i b_j | 1 \leq i \leq m, 1 \leq j \leq m\}$ είναι βάση του $[M:K]$.

Έστω L/K επέκταση σωμάτων. Ένα στοιχείο $a \in L$ θα λέγεται αλγεβρικό υπέρ το K αν και μόνο αν υπάρχει $f(x) \in K[x]$ με $f(x) \neq 0$ και $f(a) = 0$. Αν $a \in L$ όχι αλγεβρικό θα λέμε ότι το a είναι υπερβατικό.

Ορισμός 4 *Μια επέκταση L/K λέγεται αλγεβρική αν όλα τα στοιχεία της είναι αλγεβρικά.*

Θεώρημα 2 *Αν ο βαθμός $[L:K]$ είναι πεπερασμένης τάξης τότε η επέκταση L/K είναι αλγεβρική.*

Απόδειξη: Έστω $[L:K] = n$. Έστω a τυχαίο στοιχείο του L. Έστω ότι τα $1, a, a^2, a^3, ..., a^n$ δεν είναι διαφορετικά μεταξύ τους τότε υπάρχουν $0 \leq i, j \leq n$ ώστε $a^i = a^j$. Άρα $a^{(i-j)} = 1$ άρα το a είναι ρίζα του $f(x) = x^{(i-j)} - 1$. Αν τα $1, a, a^2, a^3, ..., a^n$ είναι διαφορετικά μεταξύ τους τότε είναι και γραμμικά εξαρτημένα υπέρ το K διότι είναι $n+1 > [L:K] = n$. Συνεπώς υπάρχει σχέση $\lambda_0 1 + \lambda_1 a + ... + \lambda_n a^n = 0$, $\lambda_i \in K$ όπου τουλάχιστον ένα από λ_i είναι διάφορο του μηδενός. Επομένως το a είναι αλγεβρικό ως ρίζα του πολυωνύμου $f(x) = \lambda_0 1 + \lambda_1 x + ... + \lambda_n x^n$. Άρα η επέκταση $[L:K]$ είναι αλγεβρική.

Θεώρημα 3 *Έστω L/K όχι πεπερασμένη επέκταση, και*

$$L' = \{a \in L | a \text{ αλγεβρικό υπέρ το } K\}.$$

Τότε το L' είναι υπόσωμα του L.

Απόδειξη: Έστω $a \neq 0$ και $b \in L'$. Συμβολίζουμε με $K_{(a,b)}/K$ την επέκταση η οποία περιέχει όλα τα στοιχεία της μορφής $f(a,b)$ όπου $f \in K(x,y)$. Η επέκταση $K_{(a,b)}/K$ είναι πεπερασμένη άρα αλγεβρική. Άρα $a-b, ab$ και a^{-1} αλγεβρικά υπέρ το K. Συνεπώς $a-b, ab$ και $a^{-1} \in L'$. Επομένως το L' είναι σώμα.

Ορισμός 5 *Το L' λέγεται αλγεβρική θήκη του K στο L.*

Πρόταση 1 *Αν $a \in L$, a αλγεβρικό υπέρ το L' τότε $a \in L'$.*

Απόδειξη: Η επέκταση $L'_{(a)}/L'$ είναι πεπερασμένη άρα και αλγεβρική. Επίσης η L'/K είναι αλγεβρική. Επομένως $L'_{(a)}/K$ είναι αλγεβρική. Συνεπώς το a είναι αλγεβρικό υπέρ το K. Άρα $a \in L'$.

Δηλαδή, όπως λέμε το L' είναι αλγεβρικά κλειστό στο L.

Ορισμός 6 *Έστω Ω σώμα . Το Ω λέγεται αλγεβρικά κλειστό όταν και μόνο όταν για κάθε $f(x) \in \Omega[x]$ με $\deg f(x) > 0$, υπάρχει τουλάχιστο μία ρίζα a του $f(x)$ τέτοια ώστε $a \in \Omega$.*

Θεμελιώδες θεώρημα της άλγεβρας: το $\mathbb{C}$ είναι αλγεβρικά κλειστό.[1].

Πρόταση 2 *Έστω σώμα $K \subset \Omega$, Ω αλγεβρικά κλειστό. Τότε η αλγεβρική θήκη $\tilde{K}$ του K στο Ω είναι επίσης αλγεβρικά κλειστό σώμα.*

Απόδειξη: Έστω $f(x) \in \tilde{K}[x]$, $\deg f(x) > 0$. Συνεπώς $f(x) \in \Omega[x]$ και επομένως το $f(x)$ έχει όλες τις ρίζες του $a_1, a_2, ..., a_n$ στο Ω. Δηλαδή τα $a_1, a_2, ..., a_n \in \Omega$ και είναι αλγεβρικά υπέρ το $\tilde{K}$. Άρα $a_i \in \tilde{K}$.

Ορισμός 7 *Το L λέγεται αλγεβρική θήκη του K αν και μόνο αν:*

- *Το L είναι αλγεβρικά κλειστό και*
- *Η επέκταση L/K είναι αλγεβρική.*

Τέλος πρέπει να αναφερθεί ότι για κάθε σώμα K υπάρχει μια αλγεβρική θήκη αυτού L η οποία είναι μοναδική μέχρι ισομορφίας. Δηλαδή μπορεί να υπάρχει και άλλο σώμα τέτοιο ώστε να αποτελεί αλγεβρική θήκη του K αλλά τότε αυτό θα είναι ισόμορφο με το L.

Εφαρμογή: Πεπερασμένα σώματα

Έστω p πρώτος, το σύνολο των κλάσεων ισοδυναμίας mod$p$ αποτελεί σώμα το οποίο θα το γράφουμε $\mathbb{F}_p$

Θεώρημα 4 *Αν q είναι δύναμη πρώτου, $q = p^s$, τότε υπάρχει ένα σώμα με q στοιχεία το οποίο θα το συμβολίζω με $\mathbb{F}_q$, και το σώμα αυτό προκύπτει σαν αλγεβρική επέκταση του $\mathbb{F}_p$ βαθμού s.*

Απόδειξη: Η απόδειξη υπάρχει στο [8]

1.2 Ρητά σημεία επιπέδων καμπυλών

Ένα σημείο στο (x, y)-επίπεδο καλείται ρητό σημείο αν και μόνο αν οι συντεταγμένες του x και y είναι ρητοί αριθμοί.

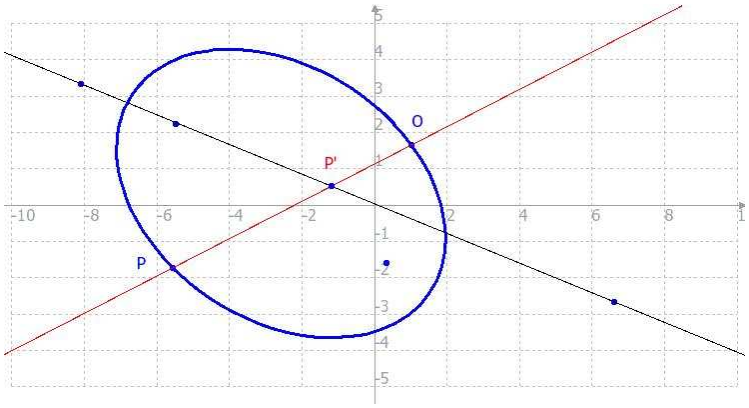
Μια ευθεία θα λέγεται ρητή αν η εξίσωση της μπορεί να γραφτεί με ρητούς συντελεστές, δηλαδή όταν η εξίσωση της είναι της μορφής

$$ax + by + c = 0, \qquad a, b, c \in \mathbb{Q}$$

Παρατήρηση:

1. Αν $(x_1, y_1), (x_2, y_2)$ είναι ρητά σημεία του επιπέδου τότε και η ευθεία που ορίζουν είναι επίσης ρητή.
2. Δύο ρητές ευθείες τέμνονται σε ρητό σημείο. Αν $y = a_1x + b_1, y = a_2x + b_2$ τότε αν $a_1 \neq a_2$ το σημείο τομής τους είναι το $(\frac{b_2 - b_1}{a_1 - a_2}, \frac{b_2a_1 - a_2b_1}{a_1 - a_2})$ το οποίο είναι ρητό.

[1] Το θεμελιώδες θεώρημα της άλγεβρας αποδείχθηκε από τον Gauss στην διδακτορική του διατριβή, η οποία είχε τίτλο «Μια νέα απόδειξη του θεμελιώδους θεωρήματος της άλγεβρας ». Κι όμως ο Gauss έκανε λάθος, δεν ήταν μια νέα απόδειξη αλλά η πρώτη. Για μια απόδειξη του Θεμελιώδους Θεωρήματος της Άλγεβρας με χρήση μιγαδικών συναρτήσεων παραπέμπουμε στο [9]



Σχήμα 1.1: Ρητή παραμετρικοποίηση κωνικής τομής

1.3 Κωνικές τομές με δοσμένο ρητό σημείο

Κωνική τομή είναι η καμπύλη που προκύπτει από την τομή επιπέδου με κώνο. Η γενική εξίσωση κάθε κωνικής τομής δίνεται από τον τύπο:

$$ax^2 + bxy + cy^2 + dx + ey + f = 0,$$

Αν η εξίσωση μπορεί να γραφεί με συντελεστές a, b, c, d, e, f ρητούς αριθμούς τότε θα λέγεται ρητή.

Αν ένα από τα δύο σημεία τομής μιας ρητής κωνικής τομής με ρητή ευθεία είναι ρητό σημείο τότε και το άλλο σημείο τομής είναι επίσης ρητό.

Αυτό το βλέπουμε λύνοντας το σύστημα κωνικής τομής και ευθείας (αντικαθιστούμε το y της ευθείας στην κωνική τομή). Έτσι βρίσκουμε μια δευτεροβάθμια εξίσωση ως προς x έστω $Ax^2 + Bx + C = 0$. Αν η κωνική τομή και η ευθεία είναι ρητές, τότε $A, B, C \in \mathbb{Q}$. Το x ανήκει εν γένει σε αλγεβρική επέκταση του $\mathbb{Q}$ βαθμού δύο γιατί αν το x είναι άρρητος τότε ανήκει στο $\mathbb{Q}_{(x)}$. Προφανώς αν x είναι ρητός τότε και ο y είναι ρητός. Το πρόβλημα λοιπόν είναι ισοδύναμο με το ότι αν μια δευτεροβάθμια εξίσωση με ρητούς συντελεστές έχει μια ρητή λύση τότε και η άλλη λύση της θα είναι ρητή. Αν $x_1 = \frac{-B+\sqrt{\Delta}}{2A}$ είναι μια ρητή ρίζα τότε αφού $2A$ ρητός, συνεπάγεται ότι και $(-B + \sqrt{\Delta})$ ρητός. Άρα και ο $(-B - \sqrt{\Delta})$ είναι ρητός και άρα $x_2 = \frac{-B-\sqrt{\Delta}}{2A}$ ρητός. Το ίδιο ισχύει και αντίστροφα.

Εγκαταλείπουμε προς στιγμήν το ερώτημα της ύπαρξης ενός ρητού σημείου, υποθέτουμε ότι το O είναι ένα ρητό σημείο κωνικής τομής και θα δούμε πώς μπορούμε να βρούμε όλα τα ρητά σημεία αυτής. Παίρνουμε μια ρητή ευθεία L και προβάλουμε την κωνική τομή C πάνω στην ευθεία L από το σημείο O. Έτσι έχουμε μια ένα προς ένα αντιστοιχία ανάμεσα στα σημεία της κωνικής τομής P που είναι διάφορα του O και στα σημεία της ευθείας L. Αφού το O είναι εξ υποθέσεως ρητό σημείο, το P είναι ρητό αν και μόνο αν το Q είναι ρητό. (Διότι αν κατ'αρχάς το P είναι ρητό, η ευθεία OP είναι ρητή και επομένως η τομή των ευθειών OP και L είναι ρητό σημείο. Αν τώρα το Q είναι ρητό σημείο , η ευθεία OQ είναι ρητή

και επειδή η κωνική τομή C είναι ρητή και το ένα σημείο τομής, το O είναι ρητό έπεται ότι και το άλλο σημείο τομής το Q θα είναι επίσης ρητό).

Ώστε, τα ρητά σημεία της κωνικής τομής C, τα διάφορα του O βρίσκονται σε ένα προς ένα αντιστοιχία με τα ρητά σημεία της γραμμής L.

Παράδειγμα. Έστω η κωνική τομή (κύκλος) $x^2 + y^2 = 1$ Σχήμα 2.2. Προβάλουμε κάθε σημείο (x, y) του κύκλου στον άξονα των y, από το ρητό σημείο $(-1, 0)$. Η ευθεία που περνά από τα σημεία $(-1, 0)$ και $(0, t)$ $t \in \mathbb{R}$ έχει εξίσωση $y = t(1 + x)$, οπότε το σύστημα των εξισώσεων

$$x^2 + y^2 = 1$$

και

$$y = t(1 + x)$$

μας δίνει ότι $t^2(1 + x)^2 + x^2 = 1$, $t^2(x^2 + 2x + 1) + x^2 = 1$ και επομένως $(1 + t^2)x^2 + 2t^2x + t^2 - 1 = 0$. Το πολυώνυμο αυτό έχει διακρίνουσα $\Delta = 4t^4 - 4(t^2 - 1)(t^2 + 1) = 4$. Συνεπώς παίρνουμε τις λύσεις:

$$x = \frac{1-t^2}{1+t^2}, \text{ και } x = -1.$$

Η δεύτερη λύση αντιστοιχεί στο σημείο $(-1, 0)$. Άρα οι λύσεις (x, y) του παραπάνω συστήματος δίνονται από την παραμετρική μορφή

$$x = \frac{1-t^2}{1+t^2}, \text{ και } y = \frac{2t}{1+t^2}.$$

Παρατηρούμε ότι το t είναι ρητός τότε και μόνο τότε όταν το (x, y) είναι ρητό σημείο του κύκλου.

Αν θέλουμε να πάρουμε και το σημείο $(-1, 0)$ θα πρέπει να «αντικαταστήσουμε» το t με το άπειρο.

1.4 Ρητά σημεία κυβικών καμπυλών

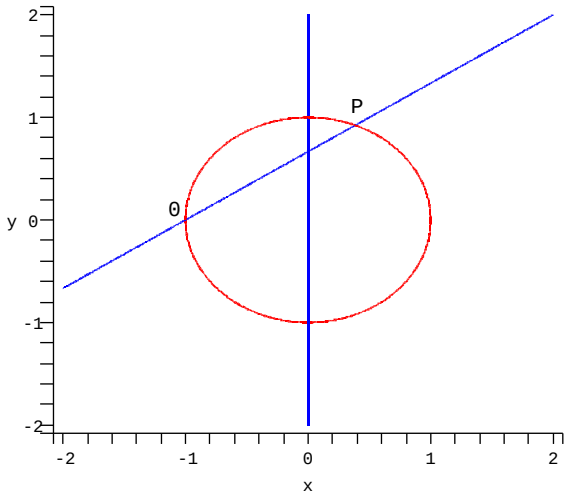
Η γενική κυβική εξίσωση έχει μορφή

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0$$

Υποθέτουμε ότι είναι ρητή, δηλαδή ότι οι συντελεστές $a, b, c, d, e, f, g, i, j$ είναι ρητοί αριθμοί.

Το πιο απλό παράδειγμα κυβικής καμπύλης χωρίς ρητό σημείο είναι ίσως η καμπύλη $x^3 + y^3 = 1$. Το να έχει η παραπάνω εξίσωση ρητά σημεία είναι ισοδύναμο με την ύπαρξη ακεραίου σημείου στην εξίσωση $x^3 + y^3 = z^3$. Αν $x^3 + y^3 = 1$ έχει ρητή λύση $(\frac{a}{b}, \frac{c}{d})$, $a, c \in \mathbb{Z}$ $b, d \in \mathbb{N}$ τότε $(\frac{a}{b})^3 + (\frac{c}{d})^3 = 1 \Rightarrow (ad)^3 + (cb)^3 = (bd)^3 \Rightarrow x^3 + y^3 = z^3$ έχει μη τετριμμένη λύση. Αντίστροφα αν $x^3 + y^3 = z^3$ έχει μη τετριμμένη ακέραια λύση τότε διαιρώντας με το z^3 συνεπάγεται ότι και η $x^3 + y^3 = 1$ έχει ρητή λύση. Το ότι η $x^3 + y^3 = z^3$ εξίσωση δεν έχει, μη τετριμμένη ακέραια λύση είναι γνωστό. (εικασία του Fermat για εκθέτη 3)

Σκοπός μας είναι να περιγράψουμε τα ρητά σημεία ρητής κυβικής καμπύλης όταν μας δίνεται ένα ρητό σημείο αυτής.



Σχήμα 1.2: Ρητή παραμετρικοποίση κύκλου.

Ξαναχρησιμοποιούμε το ίδιο γεωμετρικό αξίωμα θεωρώντας την τομή κωνικής τομής και ευθείας.

Αφού η $x-$συνιστώσα του σημείου τομής πληρεί μια κυβική εξίσωση ως προς x, έπεται ότι θα υπάρχουν τρία σημεία τομής. Εδώ δεν ισχύει ότι τα σημεία τομής ρητής κυβικής καμπύλης και ρητής ευθείας η οποία περνάει από ρητό σημείο της καμπύλης είναι επίσης ρητά(π.χ. $y^2 = (x^2-2)(x-2)$ και $y = 0$ τέμνονται στο ρητό $(2, 0)$ αλλά και στο $(\sqrt{2}, 0)$). Ισχύει όμως ότι αν δύο από τα τρία σημεία τομής μιας ρητής κυβικής καμπύλης με μια ρητή ευθεία είναι ρητά, τότε και το τρίτο είναι ρητό. Αυτό είναι ισοδύναμο με το αν μια εξίσωση τρίτου βαθμού έχει 2 ρητές ρίζες τότε και η τρίτη θα είναι ρητή. Έστω ότι $x^3 + ax^2 + bx + c = 0$ ρητή και έστω ότι έχει 2 ρητές ρίζες x_1, x_2 τότε μπορεί να γραφτεί $d(x - x_1)(x - x_2)(x - x_3) = 0$ αν το x_3 είναι άρρητος τότε αν κάνουμε τους πολλαπλασιασμούς και τη φέρουμε στην αρχική μορφή θα έχουμε πολλαπλασιασμό ρητού επί άρρητου και άρα άρρητο συντελεστή, άτοπο.

Ορισμός 8 *Έστω C ανάγωγη (δεν αναλύεται σε γινόμενο πολυωνύμων μικρότερου βαθμού) κυβική καμπύλη. Ένα σημείο O αυτής θα λέγεται ιδιάζον (singular) όταν κάθε ευθεία που περνά από το O τέμνει τη C το πολύ σε ένα σημείο με μετρημένη την πολλαπλότητα.*

Θεώρημα 5 *Αν $f(x, y)$ έχει βαθμό n και $g(x, y)$ έχει βαθμό m και δεν έχουν κοινό διαιρέτη τότε οι καμπύλες που ορίζουν τέμνονται το πολύ σε mn σημεία, με μετρημένη την πολλαπλότητα.*

Ορισμός 9 *Έστω (x_0, y_0) σημείο της καμπύλης $f(x, y) = 0$. Αν $\nabla f(x_0, y_0) \neq 0$ τότε μπορούμε να ορίσουμε τον εφαπτόμενο χώρο στο σημείο (x_0, y_0). Εφαπτόμε-*

νος χώρος στο (x_0, y_0) είναι η ευθεία που είναι κάθετη στο $\nabla f(x_0, y_0)$ και περνάει από το (x_0, y_0).

Ορισμός πολλαπλότητας σημείου με ευθεία.

Έστω $f(x, y)$ πολυώνυμο που ορίζει επίπεδη αλγεβρική καμπύλη, και έστω $p = (x_0, y_0)$ ώστε $f(x_0, y_0) = 0$

Θεωρώ την ευθεία

$$x(t) = ta + x_0, y(t) = tb + y_0$$

που περνάει από το (x_0, y_0)

Κάνοντας χρήση του τύπου του Taylor για πολλές μεταβλητές έχουμε

$$f(x(t), y(t)) = f(x_0, y_0) + \nabla f(x_0, y_0) \begin{pmatrix} at \\ bt \end{pmatrix} + \text{όροι μεγαλύτερης τάξης}$$

το οποίο είναι πολυώνυμο του t.

Ορίζω σαν πολλαπλότητα τομής της ευθείας με καμπύλη που ορίζει η f να είναι η μεγαλύτερη δύναμη του t που διαιρεί το $f(x(t), y(t))$.

Αν το $\nabla f(x_0, y_0) \neq (0, 0)$ τότε για όλες τις ευθείες πλην της εφαπτομένης, η πολλαπλότητα τομής της ευθείας είναι 1. Αν το $\nabla f(x_0, y_0) = (0, 0)$ τότε όλες οι ευθείες τέμνουν με πολλαπλότητα τουλάχιστον 2 και το πολύ 3, γιατί στο $f(x(t), y(t))$ έχουν μηδενιστεί και ο σταθερός όρος αλλά και ο όρος τάξης 1. Σε αυτή την περίπτωση αφού η ευθεία τέμνει σε 3 το πολύ σημεία με μετρημένη την πολλαπλότητα έχουμε την ισοδυναμία του ορισμού της ιδιομορφίας όπως ορίστηκε παραπάνω, με τον ακόλουθο ορισμό.

Ορισμός 10 *Μια καμπύλη θα είναι ιδιόμορφη στο (x_0, y_0) που την ικανοποιεί αν και μόνο αν $\nabla f(x_0, y_0) = (0, 0)$. Το (x_0, y_0) είναι το ιδιάζον σημείο που αναφέραμε πιο πάνω.*

Δηλαδή σε ένα ιδιάζον σημείο δεν μπορούμε να ορίσουμε εφαπτόμενο χώρο.

Παραδείγματα

- Ιδιομορφία τύπου ακίδας (Σχήμα 2.3). Έστω η συνάρτηση $f(x, y) = x^2 - y^3$ το $(0, 0)$ είναι σημείο που την επαληθεύει

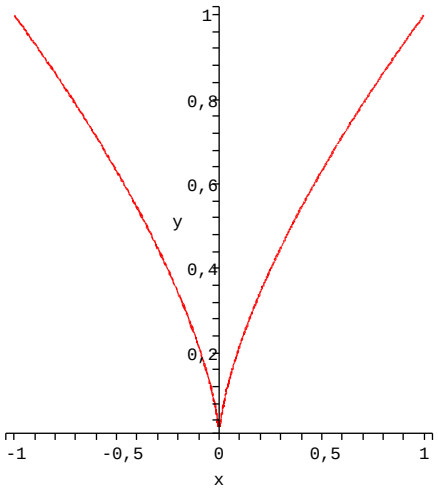
  $$\frac{\partial f}{\partial x} = 2x \qquad \frac{\partial f}{\partial y} = -3y^2 \Rightarrow \nabla f_{(0,0)} = (0, 0)$$

  Αυτό δεν ορίζει κατεύθυνση. Η καμπύλη έχει ιδιομορφία.

- Έστω η συνάρτηση $f(x, y) = x^2 + y^2 + 1$ η οποία ορίζει ένα κύκλο στο επίπεδο. Το σημείο $(0, 1)$ είναι σημείο του κύκλου.

  $$\frac{\partial f}{\partial x} = 2x \qquad \frac{\partial f}{\partial y} = 2y \Rightarrow \nabla f_{(0,1)} = (0, 2) \neq (0, 0)$$

  άρα το σημείο $(0, 1)$ είναι μη ιδιάζον.



Σχήμα 1.3: Ιδιομορφία τύπου «ακίδας».

- Έστω η συνάρτηση $f(x,y) = x^2 - y^3$. Για $x = 0 \Rightarrow y = 0$ για να ισχύει ότι $f(x,y) = 0$. Αν $y < 0$, τότε $y^3 < 0$ άρα στο $\mathbb{R}$ δεν υπάρχει x τέτοιο ώστε $x^2 - y^3 = 0$. Αν $y > 0$, $x = \pm y^{\frac{3}{2}}$ άρα το μόνο ιδιάζον σημείο που έχει η καμπύλη είναι το $(0,0)$.

- Κομβική ιδιομορφία (Σχήμα 2.4). Έστω η συνάρτηση $f(x,y) = y^2 - x(x-1)^2$ τότε $y = 0$ αν $x = 0$ ή $x = 1$. Αν $x < 0 \Rightarrow x(x-1)^2 < 0$ αρα δεν υπάρχει y που να την ικανοποιεί. Αν $x > 0$ τότε έχω δυο $y = \pm\sqrt{x(x-1)^2}$.

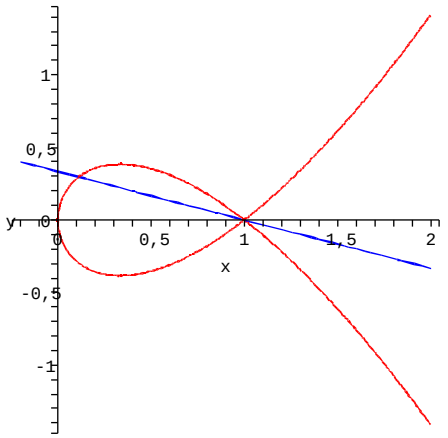
  Έστω L ρητή ευθεία που περνά από το O και τέμνει την καμπύλη σε ακριβώς ένα σημείο, έστω P. Δηλαδή το O είναι ιδιόμορφο. Προφανώς το P είναι επίσης ρητό σημείο της καμπύλης.

  Έτσι, όπως και στις κωνικές τομές, προβάλουμε την C σε κάποια ρητή ευθεία M τα ρητά σημεία της οποίας αντιστοιχούν ένα προς ένα στα ρητά σημεία της καμπύλης τα διάφορα του O.

Έστω τώρα C μη ιδιάζουσα ρητή κυβική καμπύλη. Δεν μπορούμε να χαρακτηρίσουμε τα ρητά σημεία αν μας δίνεται μόνο ένα ρητό σημείο.

Προσεγγίζουμε λοιπόν το θέμα μας αλλιώς. Παρατηρούμε ότι αν βρούμε δύο ρητά σημεία πάνω στην καμπύλη ορίζεται με τον ακόλουθο τρόπο και ένα τρίτο. Αρκεί να συνδέσουμε τα δύο σημεία με την ευθεία που ορίζουν. Το τρίτο σημείο θα είναι το τρίτο σημείο τομής της ευθείας αυτής με την κυβική καμπύλη.

Προφανώς η ευθεία L είναι ρητή και τέμνει την καμπύλη σε ένα ακόμα σημείο, έστω PQ, που είναι επίσης ρητό. Αυτό είναι κάποιο είδος σύνθεσης δύο σημείων.



Σχήμα 1.4: Ρητή παραμετρικοποίηση καμπύλης με κομβική ιδιομορφία.

Ακόμη και ένα ρητό σημείο να έχει η καμπύλη, P , φέρνουμε την εφαπτομένη στο P και έχουμε ένα άλλο ρητό σημείο, το PP , (δηλαδή συνδέουμε το P με τον εαυτό του). Όμοια το PP είναι επίσης ρητό

Από δύο ρητά σημεία μπορούμε παράγουμε ένα τρίτο.

Ο νόμος της σύνθεσης που περιγράφτηκε πιο πάνω ονομάζεται *μέθοδος της χορδής και της εφαπτομένης*. Δυστυχώς με τον παραπάνω τρόπο σύνθεσης, δεν μπορούμε να εφοδιάσουμε το σύνολο των ρητών σημείων της καμπύλης με κάποια δομή. Εύκολα βλέπουμε ότι δεν αποτελεί, παραδείγματος χάριν, ομάδα, διότι δεν υπάρχει ουδέτερο σημείο, O τέτοιο ώστε $OP = P$ για όλα τα P. Αυτό μπορούμε να το επιτύχουμε με κατάλληλη τροποποίηση της μεθόδου της χορδής και της εφαπτομένης.

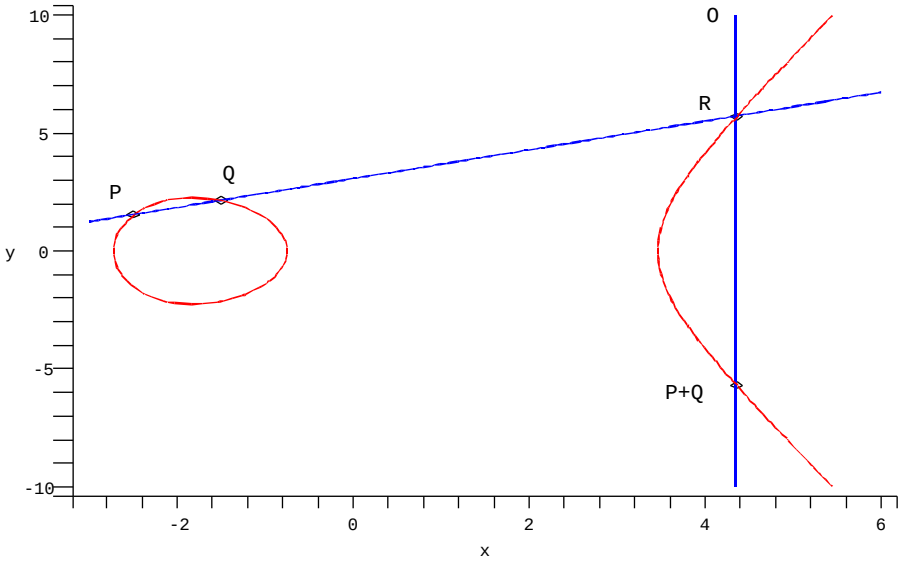
Ορισμός 11 *Έστω O ένα ρητό σημείο μιας κυβικής καμπύλης. Αν P και Q δύο οποιαδήποτε ρητά σημεία αυτής τότε «άθροισμα» τον P και Q ορίζεται να είναι το τρίτο σημείο τομής της ευθείας O, PQ με την καμπύλη.*

Το να διαπιστώσει κανείς ότι η παραπάνω ορισθείσα πρόσθεση είναι αντιμεταθετική, ότι το O είναι ουδέτερο στοιχείο ως προς την πρόσθεση και ότι κάθε ρητό σημείο της καμπύλης έχει επίσης ρητό αντίθετο, είναι σχετικά εύκολο. Το δύσκολο είναι να δείξει κανείς ότι η πράξη είναι προσεταιριστική. Όλα τα παραπάνω θα μελετηθούν στη συνέχεια.

Σημείωση. Αν P, Q, R τρία σημεία πάνω σε μια ευθεία τότε $P + Q + R = O$.

1.5 Απαλείφουσα δύο πολυωνύμων

Πρόταση 3 *Οι παρακάτω προτάσεις είναι μεταξύ τους ισοδύναμες.*



Σχήμα 1.5: Ο νόμος ομάδας σε μη ιδιόμορφη κυβική καμπύλη

1. *Το σώμα K είναι αλγεβρικά κλειστό.*
2. *Κάθε πολυώνυμο $f(x) \in K[x]$ με $\deg f(x) > 0$ αναλύεται στο K σε γινόμενο πολυωνύμων πρώτου βαθμού.*
3. *Κάθε ανάγωγο πολυώνυμο $f(x) \in K[x]$ με $\deg f(x) > 0$ είναι γραμμικό.*
4. *Αν L/K είναι αλγεβρική επέκταση τότε, κατάνάγκη, $L = K$.*

Απόδειξη: (1) $\Rightarrow$ (2) Αφού K αλγεβρικά κλειστό, έπεται οτι το $f(x)$ έχει μια ρίζα στο K, έστω a. Το $f(x)$ επομένως γράφεται $f(x) = (x-a)g(x)$ όπου $g(x) \in K[x]$. Αν $\deg g(x) > 1$, επαναλαμβάνουμε την ίδια διαδικασία για το $g(x)$ και συνεχίζουμε.

(2) $\Rightarrow$ (3):Προφανές (Αν το $f(x)$ δεν είναι γραμμικό τότε $\deg f(x) > 1$ όμως τότε αναλύεται στο K σε γινόμενο γραμμικών παραγόντων, άρα δεν είναι ανάγωγο).

(3) $\Rightarrow$ (4): Έστω L/K μια αλγεβρική επέκταση και a οποιοδήποτε στοιχείο του L. Τότε το a είναι αλγεβρικό υπέρ του K. Αν $f(x)$ είναι το ανάγωγο πολυώνυμο του a υπεράνω του K τότε λόγο της υπόθεσης (3), το $f(x)$ θα είναι της μορφής $f(x) = x - a \in K[x]$, δηλαδή $a \in K$. Αυτό σημαίνει ότι $L \subseteq K$ και άρα $L = K$.

(4) $\Rightarrow$ (1): Έστω $f(x) \in K[x]$ και $\deg f(x) > 0$. Υπάρχει επέκταση L/K, στην οποία το $f(x)$ έχει μια ρίζα έστω a. Η επέκταση $K(a)/K$ είναι πεπερασμένη συνεπώς είναι αλγεβρική και, λόγω της υπόθεσης (4), $K(a) = K$, δηλαδή $a \in K$. Επομένως το $f(x)$ έχει τουλάχιστον μια ρίζα στο K, δηλαδή η (1) ισχύει.

Πρόταση 4 *Κάθε αλγεβρικά κλειστό σώμα περιέχει άπειρο πλήθος στοιχείων.*

Απόδειξη **Περίπτωση 1:** υποθέτουμε ότι η χαρακτηριστική του σώματος K είναι μηδέν. Θεωρούμε τον ομομορφισμό $f : \mathbb{Z} \longrightarrow K$ που στέλνει το $1 \in \mathbb{Z}$ στην μονάδα του K. Αφού η χαρακτηριστική του σώματος K είναι 0 έπεται ότι f μονομορφισμός. Άρα $\mathbb{Z} \subseteq K$. Αν θέσω $g(p/q) = f(p)/f(q)$ τότε και το $g(\mathbb{Q})$ περιέχεται ισόμορφα μέσα στο K. Το $\mathbb{Q}$ όμως έχει άπειρο πλήθος στοιχείων άρα, και το K.

Περίπτωση 2: Έστω ότι η χαρακτηριστική του σώματος K είναι p, όπου p πρώτος αριθμός. Τότε το K περιέχει ισόμορφα το πρώτο σώμα $\mathbb{F}_p = \mathbb{Z}/(p)$ των κλάσεων ισοδυναμίας $(mod p)$. Αν το K είχε πεπερασμένου πλήθους στοιχεία τότε ο βαθμός της επέκτασης $K/\mathbb{F}_p$ θα ήταν πεπερασμένος, έστω m οπότε το K θα είχε p^m στοιχεία. Τότε όμως η επέκταση του K $L = K(a)$ όπου a ρίζα του $x^{p^{m+1}} - x$, είναι πεπερασμένη επομένως αλγεβρική. Επειδή το a δεν είναι ρίζα του πολυωνύμου $x^{p^m} - x$, (άμα ήταν τότε $a^{p^m} - a = 0$ και $a^{p^{m+1}} - a = 0$ άρα $a^p = a \Rightarrow a \in \mathbb{F}_p$, άτοπο) έπεται ότι $L \supset K$ το οποίο είναι άτοπο διότι το σώμα K είναι αλγεβρικά κλειστό. Επομένως το K είναι άπειρο.

Ορισμός 12 *Ένα πολυώνυμο $f(x_1, x_2, ..., x_n) \in \mathbb{R}[x_1, ..., x_n]$ λέγεται ομογενές αν για κάθε $k \in \mathbb{R}$*

$$f(kx_1, kx_2, ..., kx_n) = k^s f(x_1, x_2, ..., x_n)$$

όπου s είναι ο βαθμός του.

Ορισμός 13 *Αν*

$$f(x_0, x_1, x_2, ..., x_n) \in R[x_0, x_1, x_2, ..., x_n]$$

ομογενές πολυώνυμο βαθμού d τέτοιο ώστε το x_0 να μην διαιρεί το f. Τότε το πολυώνυμο

$$g(x_1, x_2, ..., x_n) = f(1, x_1, x_2, ..., x_n)$$

θα λέγεται συνεταιρικό του f. Προφανώς $\deg g = d$.

Ορισμός 14 *Η απαλείφουσα δύο πολυωνύμων*

$f(x) = a_0 + a_1 x + ... + a_m x^m (a_m \neq 0)$ *και* $g(x) = b_0 + b_1 x + ... + b_n x^n (b_n \neq 0)$

με συντελεστές από το δακτύλιο R , ορίζεται σαν η ορίζουσα του $(m+n) \times (m+n)$ πίνακα

$$[R(f,g)] =$$

$$\begin{bmatrix} a_0 & a_1 & \cdots & a_m & 0 & \cdots & \cdots & 0 \\ 0 & a_0 & \cdots & a_{m-1} & a_m & \cdots & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & a_0 & a_1 & \cdots & \cdots & a_m \\ b_0 & b_1 & \cdots & b_{n-1} & b_n & 0 & \cdots & 0 \\ 0 & b_0 & \cdots & \cdots & b_{n-1} & b_n & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & b_0 & b_1 & \cdots & \cdots & \cdots & b_n \end{bmatrix}.$$

Συμβολισμός: $R(f,g) = \det(R(f,g)])$

Ορισμός 15 *: Η διακρίνουσα $D(f)$ ενός πολυωνύμου $f(x) = a_n x^n + ... + a_1 x + a_0$ ορίζεται από τη σχέση.*

$$R(f,f') = (-1)^{\frac{n(n-1)}{2}} a_n D(f),$$

όπου f' είναι η παράγωγος του f.

Παράδειγμα: Έστω το πολυώνυμο $f(x) = ax^2 + bx + c$ άρα η παράγωγος είναι $f'(x) = 2ax + b$

$$[R(f,g)]=$$

$$\begin{bmatrix} c & b & a \\ b & 2a & 0 \\ 0 & b & 2a \end{bmatrix}.$$

$$\text{Άρα } D(f(x)) = b^2 - 4ac.$$

Πρόταση 5 *: Έστω $f(x) = a_0 + a_1 x + ... + a_n x^n \in R[x]$, $a_n \neq 0$ και $g(x) = b_0 + b_1 x + ... + b_m x^m \in R[x]$, $b_m \neq 0$, όπου R δακτύλιος μονοσήμαντης ανάλυσης. Οι παρακάτω προτάσεις είναι μεταξύ τους ισοδύναμες:*

1. *Τα πολυώνυμα f και g έχουν κοινό παράγοντα διάφορο σταθεράς.*
2. *$R(f,g) = 0$*

Απόδειξη χρησιμοποιούμε το παρακάτω λήμμα:

Λήμμα 1 *Τα παρακάτω είναι ισοδύναμα.*

- *το (1) της παραπάνω πρότασης*
- *υπάρχουν μη τετριμμένα πολυώνυμα φ και ψ βαθμού μικρότερου από n και m αντίστοιχα έτσι ώστε $\psi f = \varphi g$*

Απόδειξη $\Rightarrow$)
Έστω $f = h\varphi$, $g = h\psi$. Τότε $h\varphi\psi = h\varphi\psi$ και επομένως $f\psi = \varphi g$. Αφού $\deg h > 0$ έπεται ότι $\deg\varphi < n$ και $\deg\psi < m$.

$\Leftarrow$) Έστω ότι $\psi f = \varphi g$. Αναλύουμε το g σε γινόμενο πρώτων παραγόντων. Οι διάφοροι σταθεράς παράγοντες του g, ή οι συνεταιρικοί τους, περιέχονται στους πρώτους παράγοντες του ψf. Όμως δεν μπορούν να εμφανίζονται όλοι σαν παράγοντες του ψ διότι $\deg\psi < \deg g$. Συνεπώς υπάρχει τουλάχιστον ένας πρώτος παράγοντας του g που είναι και παράγοντας του f. Άρα $g = hg'$ και $g = hg'$

απόδειξη της πρότασης 5 $\Rightarrow$ Από το λήμμα έχουμε $\psi f = \varphi g$. Εστω

$$\varphi(x) = c_1 x + ... + c_n x^{n-1} \in R[x],$$

και

$$\psi(x) = d_1 x + ... + d_m x^{m-1} \in R[x]$$

όπου ένα τουλάχιστο $c_i \neq 0$ και ένα τουλάχιστο $d_j \neq 0$. Η εξίσωση $\psi f = \varphi g$ τότε γράφεται

$$a_0 d_1 = b_0 c_1$$
$$a_1 d_1 + a_0 d_2 = b_1 c_1 + b_0 c_2$$
$$\ldots\ldots\ldots\ldots\ldots$$
$$a_n d_m = b_m c_n$$

Έχουμε δηλαδή ένα ομογενές και γραμμικό σύστημα ως προς τις $(n+m)$ μεταβλητές

$$c_1, c_2 \ldots., c_n, d_1, d_2 \ldots., d_m .$$

Το σύστημα έχει μη τετριμμένη λύση. Συνεπώς η ορίζουσα των συντελεστών πρέπει να είναι μηδέν.

Άρα $R(f,g) = 0$.

$\Leftarrow$)

Αν $R(f,g) = 0$ τότε το παραπάνω σύστημα έχει μη τετριμμένη λύση στο σώμα πηλίκων F του R (το σώμα πηλίκων μιας ακέραιας περιοχής είναι το μικρότερο δυνατό σώμα το οποίο περιέχει την ακέραια περιοχή). Πολλαπλασιάζουμε με τον κοινό παρανομαστή όλων τον όρων τον εξισώσεων του συστήματος και σχηματίζουμε σύστημα στο R που έχει τουλάχιστο ένα από τα $c_i \neq 0$ ή ένα απο τα $d_j \neq 0$. Αν $c_i \neq 0$τότε $\varphi \neq 0$ οπότε, από τη σχέση $f\psi = g\varphi$, έπεται ότι και $\psi \neq 0$ και το ζητούμενο προκύπτει από το παραπάνω λήμμα.

Πρόταση 6 *Κάθε παράγοντας ομογενούς πολυωνύμου*

$$f(x_0, x_1, x_2, ..., x_n) \in R[x_0, x_1, x_2, ..., x_n]$$

είναι ομογενές πολυώνυμο.

Απόδειξη : Ας υποθέσουμε ότι το f αναλύεται σε γινόμενο $f = h_1 h_2$ και ότι το h_1 δεν είναι ομογενές. Αναλύουμε τα h_1 και h_2 σε αθροίσματα ομογενών

$$h_1 = H_i + H_{i+1} + ... + H_{i+j}, H_i \neq 0, H_{i+j} \neq 0, j > 0$$

$$h_2 = H'_k + H'_{k+1} + ... + H'_{k+l}, H'_k \neq 0, H'_{k+l} \neq 0, l \geq 0$$

Τότε

$$f = h_1 h_2 = H_i H'_k + (H_{i+1} H'_k + H_i H'_{k+1} + ... + H_{i+j} H'_{k+l}),$$

$$H_i H'_k \neq 0 \text{ και } H_{i+j} H'_{k+l} \neq 0.$$

$$\text{Αλλά } \deg H_i H'_k = i + k < i + j + k + l = \deg H_{i+j} H'_{k+l}.$$

Επομένως αν κάποιος παράγοντας του f δεν είναι ομογενές πολυώνυμο τότε και το f δεν θα ήταν ομογενές, άτοπο.

Άμεση συνέπεια της παραπάνω πρότασης είναι το

Πόρισμα 1 *Αν f και g είναι συνεταιρικά πολυώνυμα τότε κάθε παράγοντας του f είναι συνεταιρικός με κάποιο παράγοντα του g και αντιστρόφως.*

Ειδικά: Το f είναι ανάγωγο αν και μόνο εάν το g είναι ανάγωγο.

Πρόταση 7 *Τα ομογενή πολυώνυμα*

$$F_1(x_0, x_1) = a_0 x_0^n + a_1 x_0^{n-1} x_1 + ... + a_n x_1^n \in R[x_0, x_1]$$

$$F_2(x_0, x_1) = b_0 x_0^m + b_1 x_0^{m-1} x_1 + ... + b_m x_1^m \in R[x_0, x_1]$$

έχουν κοινό παράγοντα διάφορο σταθεράς ακριβώς τότε όταν η απαλείφουσα $R(F_1, F_2) = 0$.

Απόδειξη : Αν $a_n = b_m = 0$ τότε $R(F_1, F_2) = 0$. Επειδή η τελευταία στήλη του πίνακα της απαλείφουσας θα έχει όλο μηδενικά. Έπεται τότε ότι F_1 και F_2 θα έχουν κοινό παράγοντα το x_0.

Αν $a_n b_m \neq 0$ παίρνουμε τα συνεταιρικά των F_1 και F_2 g_1 και g_2. Η πρόταση 5 και το πόρισμα 1 μας δίνουν και σε αυτή την περίπτωση την ζητούμενη ισοδυναμία.

Αν τώρα $a_n = 0$ και $b_m \neq 0$ τότε $F_1(x_0, x_1) = x_0^r F_1^*(x_0, x_1)$ όπου το x_0 δεν διαιρεί το F_1^*. Εφαρμόζουμε ξανά την πρόταση 5 και το πόρισμα 1 για τα F_1^* και F_2 και έχουμε ότι τα F_1^* και F_2 έχουν κοινό παράγοντα διάφορο σταθεράς ακριβώς τότε όταν $R(F_1^*, F_2) = 0$. Παρατηρούμε ότι $R(F_1, F_2) = \pm b_m^r R(F_1^*, F_2)$ και συνεπώς ξανά προκύπτει το ζητούμενο. Όμοια αν $a_n \neq 0$ και $a_m = 0$.

1.6 Προβολικοί χώροι

Θεωρούμε τον τρισδιάστατο χώρο k^3. Κάθε σημείο παρίσταται με συντεταγμένες (x, y, z). Μια ευθεία γραμμή που περνάει από την αρχή των αξόνων $(0, 0, 0)$ ορίζεται μονοσήμαντα από οποιοδήποτε σημείο (x, y, z) διάφορο του $(0, 0, 0)$. Επιπλέον δύο σημεία (x, y, z) και (x', y', z') ορίζουν την ίδια ευθεία που περνάει από την αρχή $(0, 0, 0)$ τότε και μόνο τότε όταν υπάρχει μια σταθερά $a, a \neq 0$, τέτοια ώστε,

$$x' = ax, \quad y' = ay, \quad \text{και } z' = az.$$

Έστω $\mathbb{P}_2$ το σύνολο όλων των ευθειών που περνούν από την αρχή (0,0,0). Τα σημεία του $\mathbb{P}_2$, δηλαδή οι ευθείες που περνούν από την αρχή των αξόνων, μπορούν να παραμετρικοποιηθούν από τις κλάσεις ισοδυναμίας των τριάδων (x, y, z) μέσω της παραπάνω σχέσης ισοδυναμίας. Την κλάση ισοδυναμίας του (x, y, z) την συμβολίζουμε με $[x, y, z]$.

Το ερώτημα που προκύπτει είναι από ποιο σύνολο (σώμα) παίρνουμε τις συντεταγμένες x, y, z.

- Στην κλασική αναλυτική γεωμετρία είναι το $\mathbb{R}$.
- Στην κλασική αλγεβρική γεωμετρία είναι το $\mathbb{C}$.
- Σε προβλήματα ρητών σημείων είναι το $\mathbb{Q}$.

Γενικά τα x, y, z θα είναι στοιχεία ενός σώματος k και το προβολικό επίπεδο

$$\mathbb{P}_2(k) := \{[x, y, z] | x, y, z \in k, (x, y, z) \neq (0, 0, 0)\}.$$

Εμφυτεύουμε το επίπεδο k^2 στο προβολικό $\mathbb{P}_2(k)$ ως εξής

$$(x, y) \in k^2 \to [x, y, z] \in \mathbb{P}_2(k).$$

Κάθε σημείο $[x, y, z] \in \mathbb{P}_2(k)$ με $z \neq 0$ παριστά το σημείο $(\frac{x}{z}, \frac{y}{z})$ του k^2 διότι

$$[x, y, z] = [(\tfrac{x}{z}, \tfrac{y}{z}, 1)] \text{ στο } \mathbb{P}_2(k).$$

Ορίζουμε ευθεία στο $\mathbb{P}_2(k)$

$$E_{a,b,c} = \{[x, y, z] | az + bx + cy = 0, \text{όπου } (a, b, c) \neq (0, 0, 0)\}$$

Για $a = 1$, $b = 0$, $c = 0$ έχουμε $z = 0$ την επ'απειρο ευθεία, η οποία αποτελείται από όλα τα σημεία της μορφής $[x, y, 0]$.

Για $z = 1$ παίρνουμε $a + bx + cy = 0$ που είναι μια συνηθισμένη αφινική ευθεία όταν $bc \neq 0$.

Δυο σύνολα συντελεστών a, b, c και a', b', c' ορίζουν την ίδια ευθεία τότε και μόνο τότε όταν υπάρχει $u \in k, u \neq 0$ τέτοιο ώστε $a' = ua, b' = ub, c' = uc$. Έστω E η ευθεία που ορίζεται από τα a, b, c και E' από τα a', b', c'. Έστω $(x, y, z) \in E$ τότε $az+bx+cy = 0$ οπότε $uaz+ubx+ucy = 0$ άρα $(x, y, z) \in E'$. Έστω τώρα ότι $(x, y, z) \in E'$ τότε $a'z+b'x+c'y = 0$ άρα $uaz+ubx+ucy = 0 \Rightarrow az+bx+cy = 0$ άρα $(x, y, z) \in E$.

Για ένα μοντέλο του προβολικού χώρου ανεξάρτητο από το σύστημα συντεταγμένων, παίρνουμε ένα τρισδιάστατο διανυσματικό χώρο V πάνω από το k και συμβολίζουμε με $\mathbb{P}(V)$ το σύνολο όλων των μονοδιάστατων υποχώρων του V. Ας σημειωθεί ότι $\mathbb{P}_2(k) = \mathbb{P}(k^3)$.

Όμοια μπορούμε να θεωρήσουμε τον r-διάστατο προβολικό χώρο $\mathbb{P}_r(k)$ υπέρ το k. Η ισοδυναμία των σημείων δίνεται από τη σχέση

$$(y_0, y_1, ..., y_r) \approx (y_0', y_1', ..., y_r') \Leftrightarrow \exists \lambda \in k - \{0\} \text{ ώστε } y_i' = \lambda y_i,\ y_i \text{ όχι όλα } 0.$$

1.7 Εισαγωγή στις επίπεδες αλγεβρικές καμπύλες

Μέχρι στιγμής μελετήσαμε τις ευθείες στο προβολικό χώρο και είδαμε ότι έχουν εξίσωση $l(x, y, z) = 0$ όπου $l(x, y, z)$ είναι ομογενές πολυώνυμο πρώτου βαθμού.

Μια επίπεδη αλγεβρική καμπύλη C_f βαθμού d είναι το σύνολο όλων των σημείων $[x, y, z] \in \mathbb{P}_2(k)$ τέτοιων ώστε $f(x, y, z) = 0$ όπου το f είναι ομογενές πολυώνυμο βαθμού d.

Αφού για κάθε ομογενές πολυώνυμο βαθμού d ισχύει

$$f(\lambda x, \lambda y, \lambda z) = \lambda^d f(x, y, z),$$

αν για κάποιο αντιπρόσωπο (x, y, z) της κλάσης $[x, y, z]$ ισχύει $f(x, y, z) = 0$, το ίδιο θα ισχύει και για κάθε στοιχείο της κλάσης. Έτσι μπορούμε να ορίσουμε σαν προβολική καμπύλη ,που ορίζεται απο το f, το σύνολο τών στοιχείων του $\mathbb{P}_2(k)$ που μηδενίζουν την ομογενή εξίσωση f

Θέτοντας $z = 1$ στην παραπάνω εξίσωση ,μπορούμε να δούμε ένα μοντέλο της παραβολικής καμπύλης στο επίπεδο. Έστω $g(x, y) = f(x, y, 1)$. Προφανώς $deg(g(x, y)) \leq d$.

Ορίζουμε

$$C_g^{aff} = \{(x, y) \in k^2 | g(x, y) = 0.\}$$

Προφανώς, ισχύει $C_g^{aff} = C_f \cap k^2$.

Αντίστροφα αν $g(x, y)$ πολυώνυμο βαθμού μικρότερου ή ίσου με d τότε το πολυώνυμο $f(x, y, z) = z^d g(\frac{x}{z}, \frac{y}{z})$ είναι ομογενές βαθμού d και $f(x, y, 1) = g(x, y)$. Αφού $f(x, y, z) = 0 \Leftrightarrow f(x, y, z)^2 = 0$ το σύνολο των σημείων της C_f δεν ορίζει μονοσήμαντα την εξίσωση $f(x, y, z) = 0$. Αν το f έχει την ανάλυση $f = f_1 f_2 ... f_r$ τότε προφανώς ισχύει:

$$C_f = C_{f_1} \cup C_{f_2} \cup ... \cup C_{f_r}.$$

Αν πάλι $f|f'$ τότε $C_f \subset C'_f$.

Δεδομένου ότι η απάντηση στο ερώτημα πότε το πολυώνυμο f αναλύεται σε γινόμενο παραγόντων και πότε όχι εξαρτάται από το σώμα k θα μιλάμε για την επίπεδη αλγεβρική καμπύλη πάνω στο k. Τέλος, για να είμαστε σίγουροι ότι υπάρχουν αρκετά σημεία πάνω στη καμπύλη, θα παίρνουμε τις συντεταγμένες των σημείων κάθε φορά από συγκεκριμένη επέκταση K του k.

Ορισμός 16 *Μία ανάγωγη επίπεδη αλγεβρίκη καμπύλη C_f βαθμού d ορισμένη υπέρ το σώμα k ορίζεται από ένα ανάγωγο ομογενές πολυώνυμο $f(x,y,z) \in k[x,y,z]$ βαθμού d. Για να δείξουμε την εξάρτηση το Σώμα K ορίζουμε*

$$C_f(K) = \{[x,y,z] \in \mathbb{P}_2(K) | f(x,y,z) = 0.\}$$

Αν η $f = f_1^{a(1)} f_2^{a(2)} ... f_r^{a(r)}$ είναι ανάλυση του ομογενούς πολυωνύμου f βαθμού d του $k[x,y,z]$ σε γινόμενο πρώτων παραγόντων τότε ισχύει.

$$C_f(K) = C_{f_1}(K) \cup ... \cup C_{f_r}(K).$$

Η καμπύλη C_{f_i} λέγεται (ανάγωγη) συνιστώσα της C_f και ο φυσικός αριθμός $a(i)$ πολαπλότητα της C_{f_i}.

- Καμπύλες πρώτου βαθμού είναι οι ευθείες.
- Καμπύλες δευτέρου βαθμού λέγονται κωνικές τομές.
- Καμπύλες τρίτου βαθμού λέγονται κυβικές καμπύλες.
- Καμπύλες τετάρτου βαθμού λέγονται τετραδικές καμπύλες, και ούτω καθ' εξής.

Αν $K \subset K'$ επεκτάσεις του K τότε ισχύει $\mathbb{P}_2(K) \subset \mathbb{P}_2(K')$ και $C_f(K) \subset C_f(K')$

Ορισμός 17 *Μία ελλειπτική καμπύλη είναι μια μη ιδιάζουσα κυβική προβολική καμπύλη με συντελεστές από ένα σώμα η οποία έχει ένα ρητό σημείο.*

Ορισμός 18 *Μια υπερεπιφάνεια H_f στον προβολικό χώρο $\mathbb{P}_n$ ορίζεται μέσω ενός ομογενούς πολυωνύμου $f(Y_0, Y_1, ..., Y_n) \in k[Y_0, Y_1, ..., Y_n]$ βαθμού d, όπου για μια επέκταση K/k, το σύνολο $H_f(K)$ ορίζεται ως εξής*

$$H_f(K) = \{(y_0, y_1, ..., y_n) \in P_n(K) | f(y_0, y_1, ..., y_n) = 0\}.$$

Έστω τώρα

$$g(x_1, x_2, ..., x_n) = b_0 + b_1 x_n + ... + b_l x_n^l$$

όπου $l > 0$ και $b_i \in k[x_1, x_2, ..., x_{n-1}]$.

Η απαλείφουσα $R(x_1, x_2, ..., x_{n-1})$ των $g(x)$ και $g'(x)$ ως προς την μεταβλητή x_n έχει την μορφή

$$R(x_1, x_2, ..., x_{n-1}) = Ag + Bg', A, B \in k[x_1, x_2, ..., x_{n-1}, x_n]$$

Επομένως αν $g(x_1, x_2, ..., x_n) = 0$, τότε λόγω της υπόθεσης και $g'(x_1, x_2, ..., x_n) = 0$ και επομένως $R(x_1, x_2, ..., x_{n-1}) = 0$, $(x_1, x_2, ..., x_n) \in L^n$. Δηλαδή $H_g^{aff}(L) \subset H_{R(g,g')}^{aff}$. Όμως επειδή $R(g, g') \in k[x_1, x_2, ..., x_n]$ έπεται ότι $R(g, g') = 0$. Η απόδειξη είναι εντελώς ανάλογη με την απόδειξη για το g που κάναμε πιο πάνω.

Το θεώρημα 4 δίνει τώρα ότι g και g' έχουν κοινή συνιστώσα και, επειδή g ανάγωγο, θα πρέπει $g|g'$ οπότε και $f|f'$ πάνω από το $k[X]$.

Πόρισμα 2 *Έστω f και f' δυο ομογενή ανάγωγα πολυώνυμα του $k[x_1, x_2, ..., x_n]$, $\deg f > 0$ και $\deg g > 0$. Αν για κάποιο αλγεβρικά κλειστό σώμα $L, k \subset L$ και ισχύει $H_f(L) = H_{f'}(L)$ τότε $f' = cf$ όπου $c \in k - \{0\}$ και $H_f(K) = H_g(K)$ για κάθε επέκταση K του k.*

Παρατήρηση Η υπόθεση ότι το L είναι αλγεβρικά κλειστό είναι ουσιώδης. Αν π.χ. πάρουμε $K = \mathbb{Q}$ και $L = \mathbb{R}$ τότε για τα πολυώνυμα

$$f(X, Y, Z) = Z^2 + X^2 + Y^2,\ f'(X, Y, z) = Z^2 + 2X^2 + Y^2$$

έχουμε $H_f(\mathbb{R}) = H_G(\mathbb{R})$ αλλά δεν είναι το g πολλαπλάσιο του f επί σταθερά.

Θεώρημα 6 *(Bezout) Έστω C και C' επίπεδες προβολικές αλγεβρικές καμπύλες ορισμένες πάνω από ένα αλγεβρικά κλειστό σώμα, οι οποίες ορίζονται από πολυώνυμα βαθμού n και m αντίστοιχα. Οι C και C' τέμνονται σε ακριβώς nm σημεία εκτός αν έχουν κοινή συνιστώσα.*

Η απόδειξη του θεωρήματος του Bezout βασίζεται σε στοιχειώδη θεωρία τομών σε αλγεβρικές επιφάνειες, αλλά η παρουσίαση της είναι έξω από τους σκοπούς της πτυχιακής αυτής εργασίας. Ο ενδιαφερόμενος αναγνώστης για την περίπτωση $R = \mathbb{C}$ μπορεί να δει το [3] για μια απόδειξη στην περίπτωση που το σώμα είναι το $\mathbb{C}$. Για μια απόδειξη του Bezout σε τυχαίο σώμα, παραπέμπουμε στο [2].

Πόρισμα 3 *Αν δύο καμπύλες βαθμού n τέμνονται σε n^2 σημεία και mn από αυτά βρίσκονται πάνω σε μια ανάγωγη καμπύλη βαθμού m, τότε τα υπόλοιπα $n(n-m)$ βρίσκονται πάνω σε μια καμπύλη τάξης $n - m$.*

Απόδειξη : Έστω F_1, F_2 οι δύο καμπύλες βαθμού n, που τέμνονται σε n^2 σημεία και G είναι η ανάγωγη καμπύλη βαθμού m, που διέρχεται από mn από αυτά τα σημεία. Μπορούμε να βρούμε κατάλληλα λ_1, λ_2 έτσι, ώστε η καμπύλη $\lambda_1 F_1 + \lambda_2 F_2$ να διέρχεται από οποιοδήποτε δοσμένο σημείο (Αν θέλω να περνάει από το (x_0, y_0), τότε έστω ότι $F_1(x_1, y_1) = a, F_2(x_2, y_2) = b$ οπότε ψάχνω λ_1, λ_2 ώστε $\lambda_1 a + \lambda_2 b = 0$ τα οποία πάντα μπορώ να βρώ). Αν διαλέξουμε αυτό το σημειο στην G, τότε η G και η $\lambda_1 F_1 + \lambda_2 F_2$ έχουν τουλάχιστον $mn + 1$ κοινά σημεία και άρα κοινή συνιστώσα, που είναι η G, επειδή είναι ανάγωγη. Συνεπώς $\lambda_1 F_1 + \lambda_2 F_2 = GH$ και άρα η GH διέρχεται από τα n^2 σημεία. Η καμπύλη H είναι βαθμού $n - m$ και διέρχεται από τα $n(n-m)$ σημεία, από τα οποία δεν διέρχεται η G.

Θεώρημα 7 *(Θεώρημα του Pascal) Τα ζευγάρια των ευθειών που ορίζονται από τις απέναντι πλευρές ενός εξαγώνου εγγεγραμμένου σε μια ανάγωγη κωνική Q, συναντιούνται σε συνευθειακά σημεία.*

Απόδειξη : Έστω $L_1, L_2, L_3, L_4, L_5, L_6$ οι ευθείες των διαδοχικών πλευρών του εξαγώνου. Οι δύο κυβικές καμπύλες $L_1L_3L_5$, $L_2L_4L_6$ τέμνονται στις έξη κορυφές του εξαγώνου και στα τρία σημεία που θέλουμε να αποδείξουμε ότι είναι συνευθειακά. Από τα εννέα κοινά σημεία τα έξι βρίσκονται στην ανάγωγη κωνική Q, άρα τα υπόλοιπα τρία βρίσκονται σε μια ευθεία.

Θεώρημα 8 *(των εννέα σημείων) Αν δύο κυβικές καμπύλες τέμνονται σε ακριβώς 9 σημεία, τότε κάθε κυβική που διέρχεται από 8 από αυτά, διέρχεται και από το ένατο.*

Απόδειξη : Έστω F_1, F_2 είναι οι δύο κυβικές που τέμνονται στα $P_1, P_2, ..., P_9$ και F η κυβική που διέρχεται από τα σημεία $P_1, ..., P_8$. Αν η F είναι γραμμικά εξαρτημένη από τις F_1, F_2, δηλαδή $F = \lambda_1 F_1 + \lambda_2 F_2$ για κάποια λ_1, λ_2 τότε διέρχεται από το σημείο P_9 αφού οι F_1, F_2 διέρχονται από αυτό.

Αν η F είναι γραμμικά ανεξάρτητη από τις F_1, F_2 τότε μπορούμε να διαλέξουμε λ, μ, ν έτσι, ώστε η μη τετριμμένη καμπύλη $\lambda F_1 + \mu F_2 + \nu F$ να διέρχεται από οποιαδήποτε δύο δοσμένα σημεία. Αλλά αυτό θα μας οδηγήσει σε άτοπο.

1. Από τα 9 σημεία 4 δεν βρίσκονται στην ίδια ευθεία.

   Αν ήταν στην ίδια ευθεία, η ευθεία αυτή θα ήταν συνιστώσα των F_1, F_2 που είναι άτοπο. Αφού οι F_1, F_2 τέμνουν σε 9 ακριβώς σημεία.

2. Από τα 9 σημεία 7 δεν βρίσκονται στην ίδια κωνική.

   Αν ήταν στην ίδια κωνική, η κωνική αυτή (που είναι ανάγωγη, επειδή αλλιώς θα είχαμε τουλάχιστον 4 σημεία στην ίδια ευθεία, που είναι άτοπο από το (1)) θα ήταν συνιστώσα των F_1, F_2 που είναι άτοπο.

3. Από τα 8 σημεία $P_1, P_2, ..., P_8$ τρία δεν βρίσκονται στην ίδια ευθεία.

   Αν τα ήταν τα P_1, P_2, P_3 στην ευθεία L, τότε τα $P_4, ..., P_8$ βρίσκονται σε μια μοναδική κωνική Q (οποιαδήποτε 5 σημεία βρίσκονται πάνω σε μια τουλάχιστον κωνική, αφού για να καθορίσουμε μια κωνική, αρκεί να υπολογίσουμε τους 6 συντελεστές της. Αυτό μπορούμε να το κάνουμε, επειδή έχουμε 5 γραμμικές ομογενείς εξισώσεις με 6 αγνώστους. Η κωνική είναι μοναδική, γιατί αν δύο κωνικές έχουν 5 τουλάχιστον κοινά σημεία, τότε έχουν κοινή ευθεία. Αλλά οι άλλες τους συνιστώσες ευθείες έχουν ένα μόνο κοινό σημείο, άρα θα έπρεπε τα 4 σημεία να ήταν συνευθειακά, που είναι άτοπο στο (1)). Έστω A ένα άλλο σημείο της L και B ένα σημείο που δεν είναι σημείο ούτε της Q ούτε της L, τότε η καμπύλη $\lambda F_1 + \mu F_2 + \nu F$ για κατάλληλα λ, μ, ν διέρχεται από τα $A, B, P_1, ..., P_8$. Άρα έχει την L για συνιστώσα και άρα η άλλη συνιστώσα είναι η Q, που δεν περιέχει όμως το B, άτοπο.

4. Από τα 8 σημεία $P_1, P_2, ..., P_8$ έξη δεν βρίσκονται στην ίδια κωνική.

Αν ήταν τα $P_1, P_2, ..., P_6$ στην ίδια κωνική Q, τότε διαλέγοντας το A στην Q και το B ένα σημείο που δεν είναι σημείο ούτε της Q ούτε της L, η L είναι η ευθεία των P_7, P_8, καταλήγουμε σε άτοπο, όπως προηγουμένως.

Από τα προηγούμενα συμπεραίνουμε ότι 3 σημεία δεν βρίσκονται στην ίδια ευθεία και 6 σημεία στην ίδια κωνική. Αλλά τότε θεωρώντας την ευθεία L που διέρχεται από τα P_1, P_2 την κωνική Q που διέρχεται από τα $P_3, ..., P_7$ και διαλέγοντας τα σημεία A, B στην L, έχουμε άτοπο όπως προηγουμένως, μια που το P_8 δεν βρίσκεται ούτε στην Q ούτε στην L. Έτσι έχουμε εξαντλήσει όλες τις περιπτώσεις.

Πόρισμα 4 *Οι ελλειπτικές καμπύλες είναι ομάδες με ουδέτερο στοιχείο το σημείο* $O = (0, 1, 0)$ *και πράξη ορισμένη από τον κανόνα χορδής -εφαπτομένης.*

Απόδειξη : Έστω P, Q ρητά σημεία της ελλειπτικής καμπύλης. Τότε το PQ είναι το τρίτο σημείο τομής της ευθείας που περνά από τα P και Q με την ελλειπτική καμπύλη E(όπου E η ελλειπτική καμπύλη) . Επίσης με $L(PQ)$ συμβολίζουμε την ευθεία που περνά από τα P και Q.

- Η πράξη είναι κλειστή.

  Έστω P, Q σημεία της E τότε το PQ είναι επίσης ρητό επειδή η ευθεία $L(PQ)$ έχει ρητούς συντελεστές, καθώς ορίζεται από τα ρητά P και Q. Επίσης το $P + Q$ είναι ρητό καθώς η ευθεία $L(PQO)$ είναι ρητή.

- Έστω $P \in E$ τότε υπάρχει το $-P$. Το οποίο είναι το τρίτο σημείο τομής της ευθείας που συνδέει τα P, O.

- Η πράξη είναι προσεταιριστική.

  Έστω A, B, C 3 σημεία της E, έχουμε:

  1. Η ευθεία L_1 που διέρχεται απο τα A, B διέρχεται και από το AB.
  2. Η ευθεία L_2 που διέρχεται απο τα AB, O διέρχεται και από το $A + B$.
  3. Η ευθεία L_3 που διέρχεται απο τα $A + B, C$ διέρχεται και από το $(A + B)C$.
  4. Η ευθεία L_4 που διέρχεται απο τα B, C διέρχεται και από το BC.
  5. Η ευθεία L_5 που διέρχεται απο τα BC, O διέρχεται και από το $B + C$.
  6. Η ευθεία L_6 που διέρχεται απο τα $A, B + C$ διέρχεται και από το $A(B + C)$.

  Η κυβική $L_1L_3L_5$ με την E έχουν κοινά σημεία τα $A, B, AB, A+B, C, (A+B)C, BC, O, B+C$. Η κυβική $L_2L_4L_6$ διέρχεται από 8 από αυτά άρα από το θεώρημα των 9 σημείων συνεπάγεται ότι διέρχεται και από το ένατο. Άρα $(A + B)C = A(B + C)$ που συνεπάγεται $(A + B) + C = A + (B + C)$.

  Παρατήρηση Οι παραπάνω κατασκευές δουλεύουν με την προυπόθεση άτι $A \neq B \neq C$. Στην περίπτωση $A = B$ χρειαζόμαστε πιο ισχυρά εργαλεία από το θεώρημα των εννέα σημείων, προκειμένου να αποδείξουμε τον προσεταιρισμό.

1.8 Εξισώσεις Weierstrass

Κάθε κυβική καμπύλη η οποία έχει ένα ρητό σημείο υπέρ το K, μπορεί μετά από εφαρμογή κατάλληλων αμφίρητων μετασχηματισμών να να έρθει στην μορφή

$$y^2z + a_1xyz + a_3yz = x^3 + a_2x^2z + a_4xz^2 + a_6z^3$$

Στην περίπτωση δε που η χαρακτηριστική είναι διαφορετική του 2 ή του 3 έχουμε ότι η παραπάνω εξίσωση μπορεί να απλοποιηθεί περισσότερο στην

$$y^2z = x^3 + axz^2 + bz^3.$$

Το ρητό σημείο είναι το σημείο $(0, 1, 0)$. Για μια περιγραφή του αμφήρητου μετασχηματισμού παραπέμπουμε στον [4].

Παρατηρούμε ότι η καμπύλη είναι μη ιδιόμορφη αν το πολυώνυμο $f(x) = x^3 + ax2 + b$ έχει απλές ρίζες ή ισοδύναμα αν

$$\Delta f = -16(4a^3 + 27b^2) \neq 0.$$

Τις εξισώσεις που έχουν αναχθεί στην παραπάνω μορφή θα τις λέμε εξισώσεις Weierstrass.

1.9 Τρόπος πρόσθεσης σημείων της ελλειπτικής καμπύλης

Έστω η ελλειπτική καμπύλη $y^2 = x^3 + ax + b$ πάνω σε ένα σώμα K. Θεωρούμε τα μη μηδενικά σημεία $P = (x_1, y_1)$ και $Q = (x_2, y_2)$.

Αν $P \neq \pm Q$,τότε $\lambda = (y_1 - y_2)/(x_1 - x_2)$ και $\nu = y_1 - \lambda x_1$. Τότε $P + Q = (x_3, y_3)$ όπου

$$x_3 = \lambda^2 - x_1 - x_2 \text{ και } y_3 = -\lambda x_3 - \nu.$$

Αν $P = -Q$ ($x_1 = x_2$ και $y_1 = y_2$) τότε $P + Q = 0$.

Αν $P = Q$ αλλά $P \neq -Q$ τότε

$$x_3 = \frac{(x_1^2 - a) - 8bx_1}{4y_1^2}$$
$$y_3 = \frac{(3x_1^2 + a)(x_1 - x_3) - 2y_1^2}{2y_1}.$$

1.10 Ελλειπτικές καμπύλες ορισμένες πάνω από πεπερασμένα σώματα

Θεωρούμε ένα σώμα $\mathbb{F}_q$ με q στοιχεία, όπου το q είναι δύναμη πρώτου. Έστω η ελλειπτική καμπύλη

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

με $(x,y) \in \mathbb{F}_q^2$.

Παρατήρηση: Η «απόδειξη» που είναι βασισμένη στο θεώρημα των 9 σημείων αποδεικνύει ότι η δομή ομάδας αφορά κυβικές καμπύλες ορισμένες πάνω από ένα αλγεβρικά κλειστό σώμα. Αν $k \subset K$ είναι ένα υπόσωμα, τότε $E(k) \subset E(K)$ δηλαδή τα k ρητά σημεία αποτελούν ένα υποσύνολο των $E(K)$ της E. Αν το ουδέτερο του $E(K)$ ανήκει στο $E(k)$ κοιτώντας τους τύπους πρόσθεσης μπορουμε να δούμε ότι η η πράξη στο $E(k)$ είναι κλειστή, δηλαδή αν $P,Q \in E(k) \Rightarrow P+Q \in E(k)$, $-P \in E(k)$ οπότε το $E(k)$ αποτελεί υποομάδα του $E(K)$.

Είναι σαφές ότι ένα άνω φράγμα για το πλήθος των ρητών σημείων το οποίο είναι ίσο με την τάξη της ομάδας $E(\mathbb{F}_p)$ υπέρ το $\mathbb{F}_q$, της καμπύλης είναι το $2q+1$. Πράγματι κάθε x δίνει το πολύ δύο τιμές για το y, και έχουμε και το επ΄ άπειρο σημείο.

Υπάρχει μια καλύτερη εκτίμηση που αποδείχτηκε από τον Hasse την δεκαετία του 30. [2]

$$|E(k) - q - 1| \leq 2\sqrt{q}.$$

Το πλήθος των ρητών σημείων της $E(k)$ δίνεται από τον τύπο

$$E(k) = q + 1 + a_q$$

Ο αριθμός a_q στην βιβλιογραφία ονομάζεται «Frobenious trace» και η ονομασία αυτή έχει να κάνει με τα εργαλεία των Deligne, Grothendieck.

Υπάρχουν γενικά πολλοί τρόποι να εκτιμήσουμε αποτελεσματικά το a_q, θα αναφέρουμε μια μέθοδο που αν και δεν είναι η καλύτερη δυνατή υπολογιστικά, είναι αρκετά στοιχειώδης.

Θεωρούμε το μοναδικό μη τετριμμένο χαρακτήρα τάξης 2

$$\chi : \mathbb{F}_q^* \longrightarrow \{\pm 1\}$$

$$\chi(t) = \begin{cases} 1 & \text{αν το } t \text{ είναι τετράγωνο στο } \mathbb{F}_q \\ -1 & \text{αν το } t \text{ δεν είναι τετράγωνο.} \end{cases}$$

Επεκτείνουμε τον χ για $x=0$, θέτοντας $\chi(0)=0$

Στην περίπτωση που το q είναι πρώτος το $\chi(t)$ ταυτίζεται με το σύμβολο του Legendre, $\chi(t) = (\frac{t}{p})$

Υποθέτουμε ότι $p \neq 2,3$, οπότε θέλουμε να μετρήσουμε το πλήθος των ρητών σημείων στην ελλειπτική καμπύλη

$$E : y^2 = x^3 + ax + b$$

[2] Για την ιστορία αναφέρουμε ότι το 1949 ο A.Weil έκανε μια σειρά από γενικές εικασίες που αφορούν το πλήθος των ρητών σημείων πολλαπλοτήτων που ορίζονται πάνω από πεπερασμένα σώματα, οι οποίες κατά κάποια έννοια γενικεύουν την εικασία για την ζ-συνάρτηση του Riemann στο επίπεδο τών αλγεβρικών καμπύλων, και οι εικασίες αυτές γενικεύουν το παραπάνω αποτέλεσμα του Hasse.

Το 1972 ο P.Deligne χρησιμοποιώντας την Etale συνομολογία του Grothendieck απέδειξε τις εικασίες αυτές κερδίζοντας το Fields medal.

οπότε έχουμε ότι

$$E(k) = 1 + \sum_{x \in \mathbb{F}_q} \chi(f(x)) + 1 = 1 + q + \sum_{x \in \mathbb{F}_q} \chi(f(x))$$

όπου $f(x) = x^3 + ax + b$

1.11 Χρήση του gp-pari.

Το πρόγραμμα gp-pari το οποίο αναπτύχθηκε απο την ομάδα του Henri Cohen στο πανεπιστήμιο του Bordeaux μας επιτρέπει να κάνουμε υπολογισμούς με ελλειπτικές καμπύλες που ορίζονται πάνω από πεπερασμένα (και όχι μόνο!) σώματα.

Η συνάρτηση

```
ellinit([a1,a2,a3,a4,a6])
```

αρχικοποιεί την ελλειπτική καμπύλη

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

ενώ η συνάρτηση

```
ellap(e,p)
```

υπολογίζει τον αριθμό a_p και κατά συνέπεια το πλήθος των ρητών σημείων της ελλειπτικής καμπύλης.

Παράδειγμα Στο παρακάτω παράδειγμα υπολογίζουμε ότι το πλήθος των $\mathbb{F}_p$ ρητών σημείων της ελλειπτικής καμπύλης

$$E : y^2 = x^3 + 320x + 1,$$

ορισμένη πάνω από το σώμα $\mathbb{F}_p$, όπου p είναι ο 10^4 κατά σειρά πρώτος, ισούται με 105272.

```
gp > p=prime(10000)  \\Select a prime p
%1 = 104729
gp > E=ellinit([0,0,0,320,1]); \\Definition of the Elliptic Curve.
gp >ap=ellap(E,p)
%3 = -542   \\ Computation of the Frobenius trace.
p+1-ap
%4 = 105272
```

Παράδειγμα Κάνοντας χρήση του pari θα μελετήσουμε την δομή ομάδας στην καμπύλη

$$E : y^2 = x^3 + x + 1,$$

ορισμένη στο σώμα $\mathbb{F}_5$.

```
gp > E=ellinit([0,0,0,1,1]);
        gp > ap=ellap(E,p)
%3 = -3
gp > p+1-ap
%4 = 9
```

Δηλαδή η τάξη της E είναι 9. Υπάρχουν δύο δυνατότητες για αβελιανή ομάδα τάξης 9. Άρα $E(\mathbb{F}_5) \cong \mathbb{Z}_9$ ή $E(\mathbb{F}_5) \cong \mathbb{Z}_3 \times \mathbb{Z}_3$. Προκειμένου να δείξουμε ότι πρόκειται για την πρώτη περίπτωση υπολογίζουμε τις δυνάμεις του σημείου $P = [0, 1]$ της $E(\mathbb{F}_5)$.

```
gp > for(x=1,9,print(ellpow(E,[0,1]*Mod(1,5),x)))
[Mod(0, 5), Mod(1, 5)]
[Mod(4, 5), Mod(2, 5)]
[Mod(2, 5), Mod(1, 5)]
[Mod(3, 5), Mod(4, 5)]
[Mod(3, 5), Mod(1, 5)]
[Mod(2, 5), Mod(4, 5)]
[Mod(4, 5), Mod(3, 5)]
[Mod(0, 5), Mod(4, 5)]
[0]
```

Δηλαδή το σημείο P έχει τάξη 9 και η $E(\mathbb{F}_5)$ είναι κυκλική.

Κεφάλαιο 2

Κρυπτογραφία

2.1 Ιστορικά στοιχεία και κρυπτογραφία

1. **Παραδοσιακή κρυπτογραφία.** Βασίζεται σε ένα κοινό, μυστικό κλειδί των επικοινωνούντων. Όσο το δίκτυο των επικοινωνούντων διευρύνεται,τόσο το πρόβλημα ανταλλαγής κλειδιών δυσκολεύει. Το αγκάθι της παραδοσιακής κρυπτογραφίας είναι η ασφαλής ανταλλαγή κλειδιών.

2. **Διαδίκτυο.** Τη δεκαετία του 60 αρχίζει η ανάπτυξη του ARPA (=Andvanced Research Project Agency) με στόχο τη σύνδεση στρατιωτικών υπολογιστών, οι οποίοι απέχουν μεγάλες αποστάσεις μεταξύ τους. Το 1969 γεννιέται το ARPAnet, με τέσσερις συνδεδεμένους κόμβους, του οποίου εξέλιξη είναι το διαδίκτυο (1992). Η ευρύτατη χρήση από εκατοντάδες εκατομμύρια χρήστες, του διαδικτύου ανέδειξε την ανάγκη του να επικοινωνούν δύο οποιοιδήποτε χρήστες ελεύθερα και ταυτοχρόνως, δίχως να παραβιάζεται το απόρρητο της επικοινωνίας.

3. **Το πρόβλημα ασφαλούς επικοινωνίας.** Τα παραπάνω αναδεικνύουν το εξής πρόβλημα: Σε ένα εξαιρετικά πολύπλοκο δίκτυο επικοινωνούσων οντοτήτων όπου οι δίαυλοι επικοινωνίας είναι ασφαλείς, πως είναι πρακτικώς εφικτό να επικοινωνούν δυο οποιεσδήποτε οντότητες, δίχως παραβίαση του απορρήτου της επικοινωνίας;

4. **Ανταλλαγή κλειδιού.** Είναι δυνατόν δύο επικοινωνούσες οντότητες Α (Ανθή) και Β (Βίκτορας) να ανταλλάξουν κρυπτογραφικό κλειδί δίχως να «συναντηθούν»; Ναι! Το σενάριο ανταλλαγής κλειδωμένων κουτιών μας δίνει μια ένδειξη γιάυτό.

5. **Κρυπτογραφία δημοσίου κλειδιού.**Το πρόβλημα κρυπτογραφίας δημοσίου κλειδιού θα μπορούσε να περιγραφεί με τον εξής σχηματικό παραστατικό τρόπο: Σε μία αίθουσα βρίσκονται πολλά άτομα, μεταξύ των οποίων, η Ανθή και ο Βίκτορας. Η Ανθή θέλει να δώσει τον αριθμό της πιστωτικής κάρτας της στον Βίκτορα, αλλά δεν θέλει να τον μάθουν οι άλλοι. Ο Βίκτορας της

λέει μια πληροφορία φωναχτά, και απαντάει η Ανθή επίσης φωναχτά, με μια άλλη πληροφορία. Ύστερα από αυτό, ο Βίκτορας μαθαίνει τον αριθμό της πιστωτικής κάρτας της Ανθής, ενώ κανείς άλλος δεν είναι σε θέση να τον μάθει.

2.2 Ο αλγόριθμος RSA

Υλοποίηση του παραπάνω σεναρίου με τον αλγόριθμο RSA

Ο Βίκτορας επιλέγει δύο τυχαίους πολύ μεγάλους πρώτους αριθμούς p, q τους οποίους κρατά κρυφούς. Υπολογίζει τον $n = pq$ και επιλέγει έναν θετικό ακέραιο e πρώτο προς τον $\varphi(n) = (p-1)(q-1)$ (η συνάρτηση φ ονομάζεται συνάρτηση του Euler και ορίζεται: $\varphi(n) = |\mathbb{Z}_n^*|$). Λέει στην Ανθή τους n και e, δίχως να τον νοιάζει αν τους ακούσουν οι άλλοι.

Αν ο αριθμός της πιστωτικής κάρτας είναι m, τότε η Ανθή υπολογίζει το $b = m^e mod n$. Λέει στον Βίκτορα τον b, δίχως να την νοιάζει αν ακούνε και άλλοι.

Ο Βίκτορας υπολογίζει d, τέτοιο ώστε $de = 1 \mathrm{mod} \varphi(n)$ και μετά υπολογίζει $b^d mod n$. Η τιμή που βρίσκει, είναι m. Στον αλγόριθμο RSA (ο οποίος ανακαλύφθηκε το 1978 από τους Ron Rivest,Adi Shamir, Leonard Adlerman) το δημόσιο κλειδί είναι το ζευγάρι $\{pq, e\}$. Το ιδιωτικό κλειδί είναι ο αριθμός d το οποίο το κρατάμε μυστικό. Η ουσία του αλγορίθμου είναι ότι ο κακόβουλος παραβιαστής του κρυπτογραφημένου μηνύματος προκειμένου να υπολογίσει τον αντίστροφο d του e modn θα πρέπει να παραγοντοποιήσει τον αριθμό pq κάτι που είναι απελπιστικά χρονοβόρο.

Το να παραγοντοποιήσουμε ένα αριθμό με 100 ψηφία είναι σχετικά εύκολο με το σημερινό Hardware. Όμως είναι σχεδόν ανέφικτο να παραγοντοποιήσει κανείς ένα αριθμό με 200 ψηφία. Η εταιρία RSA security βάζει κάποιους διαγωνισμούς με θέμα την παραγοντοποίηση αριθμών. Η πρώτη επιτυχία σε αυτούς τους διαγωνισμούς έγινε τον αύγουστο του 1999 από μια ομάδα ερευνητών όπου για να παραγοντοποιήσουν έναν αριθμό με 155 ψηφία 512bit χρειάστηκαν σχεδόν 6 μήνες χρησιμοποιώντας τον αλγόριθμο G.N.F.S. Σήμερα η RSA secutity προσφαίρει 10.000 δολάρια για την παραγοντοποίηση ενός αριθμού με 174 ψηφία 576bit και 200.000 δολάρια για την παραγοντοποίηση ενός αριθμού με 617 ψηφία 2048bit.

2.3 Παραγοντοποίηση ακεραίου-Μέθοδος Pollard.

Ορισμός 19 *Έστω ότι ο b είναι θετικός ακέραιος. Ένας θετικός ακέραιος n είναι b λείος εάν όλες οι πρώτες δυνάμεις που διαιρούν το n είναι μικρότερες ή ίσες με το b.*

Παραδείγματα.

- Ο 30 είναι 7 λείος.
- Ο 30 είναι 5 λείος.

- Ο 4 δεν είναι 2 λείος.
- Ο 162 δεν είναι 3 λείος.

Παρατήρηση:
Αν a είναι ένας θετικός ακέραιος πρώτος προς τον n, τότε ο $a^{\phi(n)}-1$ διαιρείται με τον n δηλαδή $a^{\phi(n)} = 1 mod n$

Το a είναι στοιχείο της πολλαπλασιαστικής ομάδας G_n που έχει τάξη $\varphi(n)$ και αποτελείται από τα $\phi(n)$ στοιχεία της $\mathbb{Z}_n$, που είναι πρώτα προς τον n. Επομένως

$$a^{\phi(n)} = 1(\text{mod } n),$$

Παρατήρηση. Θεωρητικά τουλάχιστον, το πρόβλημα του να αποφασίσει κανένας αν ένας ακέραιος είναι η όχι πρώτος, είναι λυμένο ικανοποιητικά: Το 2002, οι Agrawal,kayal,Saxena του Indian Institute of technology στο Kanpur των Ινδιών απέδειξαν ότι το πρόβλημα ανήκει στην κατηγορία P, δηλαδή υπάρχει αλγόριθμος ο οποίος δίνει απάντηση σε πολυωνυμικό χρόνο.

Η μέθοδος του Pollard.

Έστω N ο θετικός ακέραιος που θέλουμε να παραγοντοποιήσουμε. Χρησιμοποιούμε την μέθοδο Pollard για να ψάξουμε για ένα μη τετριμένο παράγοντα του N. Πρώτα διαλέγουμε ένα θετικό ακέραιο B, συνήθως στην πράξη μικρότερο του 10^6. Ας υποθέσουμε ότι υπάρχει ένας πρώτος διαιρέτης p του N έτσι ώστε ο $p-1$ είναι B-λείος. Προσπαθούμε να βρούμε το p υπολογιστικά χρησιμοποιώντας την ακόλουθη τεχνική.

Εάν το a είναι ένας ακέραιος μη διαιρετός από το p τότε από την παραπάνω παρατήρηση

$$a^{p-1} = 1(\text{mod } p)$$

Αν το m πάρει την τιμή $m = \text{ΕΚΠ}(1, 2, 3..B)$, η υπόθεση μας ότι $p-1$ είναι B-λείος συνεπάγεται ότι $p-1|m$, οπότε

$$a^m = 1(\text{mod}) \ p$$

Επιπλέον

$$p|\text{ΜΚΔ}(a^m - 1, N) > 1$$

Ο $\text{ΜΚΔ}(a^m-1, N) > 1$ επειδή το p διαιρεί το N αλλά και το (a^m-1, N). Αν $\text{ΜΚΔ}(a^m-1, N) < N$ τότε επίσης $\text{ΜΚΔ}(a^m-1, N)$ είναι μη τετριμένος παράγοντας του N. Αν $\text{ΜΚΔ}(a^m-1, N) = N$, τότε $a^m = 1(mod q^r)$ για κάθε πρώτο διαιρέτη δύναμης q^r του N. Σε αυτή την περίπτωση επαναλαμβάνουμε τα παραπάνω βήματα αλλά με μια μικρότερη επιλογή του B η πιθανός με διαφορετική επιλογή του a.

Για σταθερό B, αυτός ο αλγόριθμος συνήθως βρίσκει παράγοντα του N όταν το N είναι διαιρετό από ένα πρώτο p ώστε $p-1$ να είναι B-λείος. Μόνο περίπου το $15/100$ των πρώτων p στο διάστημα από 10^{15} και $10^{15}+10^4$ είναι τέτοια ώστε

$p-1$ είναι 10^6-λείος, οπότε η μέθοδος Pollard με $B = 10^6$ ήδη αποτυγχάνει σχεδόν 85/100 των φορών στο να βρίσκει 15 ψηφία πρώτα σε αυτό το διάστημα. Δεν θα αναλύσουμε τη μέθοδο Pollard περισσότερο, εφόσον αναφέρθηκε εδώ μόνο και μόνο για να προετοιμάσει το έδαφος για την μέθοδο με ελλειπτικές καμπύλες.

Τα ακόλουθα παραδείγματα δείχνουν τη μέθοδο Pollard

1. Σε αυτό το παράδειγμα, η μέθοδος του Pollard δουλεύει άψογα. Έστω $N = 5917$. Θα δοκιμάσουμε να χρησιμοποιήσουμε τη μέθοδο Pollard με $B = 5$. Έχουμε m =ΕΚΠ(1,2,3,4,5)=60 και παίρνουμε $a = 2$. Έτσι έχουμε

$$2^{60} - 1 = 3416 mod 5917$$

Ο λόγος που παίρνουμε το $(2^{60} - 1) mod 5917$ είναι για να αποφύγουμε τις πράξεις με ένα νούμερο τόσο μεγάλο σαν το $2^{60} - 1$. Ο ΜΚΔ παραμένει ο ίδιος.

και

$$\text{ΜΚΔ}(2^{60} - 1, 5917) = \text{ΜΚΔ}(3416, 5917) = 61,$$

Ετσι το 61 είναι παράγοντας του 5917.

2. Σε αυτό το παράδειγμα θα επαναλάβουμε τον B με ένα μεγαλύτερο ακέραιο. Έστω $N = 779167$ με $B = 5$ και $a = 2$. Αρά

$$2^{60} - 1 = 710980(\text{mod} 779167),$$

και $\text{ΜΚΔ}(2^{360360} - 1, 779167) = 1$. Με $B = 15$, έχουμε m =ΕΚΠ$(1, 2, 3, .., 15) =$ 360360,

$$2^{360360} - 1 = 584876 \ (\text{mod } 779167)$$

και

$$\text{ΜΚΔ}(2^{360360} - 1, N) = 2003,$$

Επομένως ο 2003 είναι μη τετριμμένος παράγοντας του 779167.

3. Σε αυτό το παράδειγμα θα επαναλάβουμε το B με ένα μικρότερο ακέραιο. Έστω $N = 4331$ και $B = 7$, άρα m =ΕΚΠ$(1, 2, .., 7) = 420$,

$$2^{420} - 1 = 0(\text{mod} 4331)$$

και $\text{ΜΚΔ}(2^{420} - 1, 4331) = 4331$, άρα δεν πετύχαμε παράγοντα του 4331. Αν επαναλάβουμε το B με 5 η μέθοδος του Pollard δουλεύει.

$$2^{60} - 1 = 1464 \bmod 4331$$

και ΜΚΔ $(260 - 1, 4331) = 61$, επομένως παραγοντοποιήσαμε τον 4331.

4. Αυτό το παράδειγμα, με $a = 2$ δεν δουλεύει αλλά με $a = 3$ δουλεύει. Έστω $N = 187$ και $B = 15$, έτσι m =ΕΚΠ$(1, 2, ..., 15) = 360360$,

$$2^{360360} - 1 = 0 \bmod 187$$

και ΜΚΔ$(2^{360360} - 1, 187) = 187$ επομένως δεν πετυχαίνουμε παράγοντα του 187. Αν επαναλάβουμε με $a = 3$ τότε η μέθοδος του Pollard δουλεύει.

$$3^{360360} - 1 = 66 \ (\bmod 187),$$

και ΜΚΔ$(3^{360360} - 1, 187) = 11$. Επομένως $187 = 11 \times 17$

Η κλασσική μέθοδος του Pollard στηρίζεται προφανώς στο μικρό θεώρημα του Fermat, δηλαδή πίσω από τη μέθοδο είναι η πολλαπλασιαστική ομάδα $\mathbb{Z}_p^*$. Μπορούμε όμως να χρησιμοποιήσουμε και άλλες ομάδες πέρα από την $\mathbb{Z}_p^*$; Το ερώτημα αυτό μας οδηγεί στις ομάδες των ρητών σημείων ελλειπτικών καμπυλών.

2.4 Το κίνητρο για τη μέθοδο παραγοντοποίησης κάνοντας χρήση ελλειπτικών καμπύλων

Σταθεροποιούμε ένα $B \in \mathbb{Z}$. Αν $N = pq$ με p, q πρώτοι και ούτε το $p - 1$ ούτε το $q - 1$ είναι B-λεία η μέθοδος Pollard είναι απίθανο να δουλέψει.

Για παράδειγμα έστω $B = 20$ και έστω $N = 59 \times 101 = 5959$. Παρατηρούμε ότι ούτε το $59 - 1 = 2 \times 29$ ούτε το $107 - 1 = 2 \times 53$ είναι B-λεία.

$$\text{Με } m = \text{ΕΚΠ}(1, 2, 3, ..., 20) = 232792560 \text{ έχουμε}$$

$$2^m - 1 = 5944 \bmod N \text{ και}$$

$$\text{ΜΚΔ}(2^m - 1, N) = 1$$

Άρα η μέθοδος δεν δουλεύει.

Το $p - 1$ δεν είναι B-λείο για $p = 59$ ή $p = 101$. Όμως το $p - 2 = 3 \times 19$ είναι 20-λείο.

Θα θέλαμε να αντικαταστήσουμε την ομάδα $\mathbb{Z}_n^*$ με τάξη $p - 1$, με μια ομάδα τάξης $p - 2$ και να υπολογίσουμε το a^m σε αυτή την ομάδα. Αυτό κάνει η μέθοδος παραγοντοποίησης με ελλειπτικές καμπύλες. Αντικαθιστά την ομάδα $\mathbb{Z}_n^*$ με μια ελλειπτική καμπύλη E ορισμένη στο $\mathbb{F}_p$. Η τάξη μιας τέτοιας ομάδας είναι $p + 1 \pm s$ για $0 < s < 2\sqrt{p}$.

Το κέρδος είναι ότι ματαβάλοντας την E, μπορούμε να αλλάξουμε το s και συνεπώς και την τάξη της ομάδας.

2.5 Παραγοντοποίηση με χρήση ελλειπτικών καμπύλων

Η παρακάτω μέθοδος περιγράφει τον αλγόριθμο από το άρθρο του [5]

Η νέα αυτή μέθοδος αποκομήθηκε από τη μέθοδο του Pollard αντικαθιστώντας την πολλαπλασιαστική ομάδα $\mathbb{F}_p^*$ από την ομάδα σημείων πάνω σε τυχαία ελλειπτική καμπύλη. Για να βρεθεί ένας μη τετριμμένος διαιρέτης ενός πραγματικού ακεραίου αριθμού $N > 0$, αρχίζουμε διαλέγοντας μια ελλειπτική καμπύλη E πάνω από ένα δακτύλιο $\mathbb{Z}_N$, ένα σημείο P στην E με συντεταγμένες στο $\mathbb{Z}_N$ και ένα πραγματικό ακέραιο αριθμό m =ΕΚΠ$(2, 3, .., B)$. Χρησιμοποιώντας το νόμο της πρόσθεσης της καμπύλης, υπολογίζουμε το πολλαπλάσιο mP του P. Τώρα ελπίζουμε πως υπάρχει πρώτος διαιρέτης p του N για τον οποίο mP και το ουδέτερο στοιχείο O γίνονται ίδια modulo p. Αν η E δίνεται από την εξίσωση Weierstrass

$$y^2z = x^3 + axz^2 + bz^3$$

με $O = (0, 1, 0)$ τότε η παραπάνω συνθήκη είναι ισοδύναμη με το να έχουμε την τρίτη συντεταγμένη του mP διαιρετή με p. Οπότε ελπίζουμε να βρούμε ένα μη τετριμμένο παράγοντα του N υπολογίζοντας τον μέγιστο κοινό διαιρέτη αυτής της τρίτης συντεταγμένης με N.

Εάν ο παραπάνω αλγόριθμος αποτυγχάνει με μια συγκεκριμένη ελλειπτική καμπύλη E, τότε μπορούμε να κάνουμε κάτι που δεν είναι εφικτό με τη μέθοδο Pollard. Να αλλάξουμε την ομάδα, δηλαδή να εφαρμόσουμε τη μέθοδο με μια διαφορετική ελλειπτική καμπύλη E.

Ας υποθέσουμε ότι $P = (x_1, y_1)$ και $Q(x_2, y_2)$ μη μηδενικά σημεία πάνω σε μια ελλειπτική καμπύλη $y^2 = x^3 + ax + b$ και ότι $P \neq \pm Q$.

$$\text{Έστω } \lambda = (y_1 - y_2)/(x_1 - x_2) \text{ και } v = y_1 - \lambda x_1.$$

Από τις σχέσεις υπολογισμού του τρόπου πρόσθεσης σημείων ελλειπτικής καμπύλης έχουμε ότι $P + Q = (x_3, y_3)$ όπου

$$x_3 = \lambda^2 - x_1 - x_2 \text{ και } y_3 = -\lambda x_3 - v$$

Προσπαθούμε να υπολογίσουμε το mP χρησιμοποιώντας τον δυνατό αλγόριθμο. Αν κάνουμε αριθμητική mod$N$ και το $(x_1 - x_2)^{-1}$ δεν υπολογίζεται τότε ΜΚΔ$(x_1 - x_2, N) > 1$ όποτε έχουμε παραγοντοποιήσει το N.

Παραδείγματα

Για απλότητα χρησιμοποιούμε την καμπύλη με την μορφή :

$$y^2 = x^3 + ax + 1$$

στην οποία ανήκει το σημείο $P = (0, 1)$.

Αρχικά θα παραγοντοποιήσουμε τον $N = 5959$ κάνοντας χρήση ελλειπτικών καμπύλων. Έπειτα θα παραγοντοποιήσουμε ένα πολύ μεγαλύτερο πραγματικό ακέραιο αριθμό.

```
{lcmfirst(B)=
        local(L,i); L=1; for(i=2,B,L=lcm(L,i));
        return(L);
}

{ECM(N,m) = local(E);
     E= ellinit ([0,0,0,random(N),1]*Mod(1,N));
     print("E:y^2=x^3+",lift(E[4]),"x+1, P=[0,1]");
     ellpow(E,[0,1]*Mod(1,N),m);
     }

numpoints(a,p) =return (p+1 -ellap(ellinit([0,0,0,a,1]),p));

gp > B=20; N=5959;
gp > m=lcmfirst(B)
%5 = 232792560   \\ Compute lcm(2,...,N)
gp > Mod(2,N)^m-1
%6 = Mod(5944, 5959)
gp > gcd(5944,5959)
%7 = 1            \\ Pollard method fails.
\\------------------
gp > ECM(N,m)
E:y^2=x^3+4328x+1, P=[0,1]
  ***   impossible inverse modulo: Mod(101, 5959).
```

Ο αλγόριθμος υπολογισμού απέτυχε να υπολογίσει τον αντίστροφο του $101 \bmod 5959$ άρα $101|5959$.

Θα προσπαθήσουμε τώρα να παραγοντοποιήσουμε τον

$$N = 800610470601655221392794180058088102053408423$$

```
gp > N=800610470601655221392794180058088102053408423;
gp > ECM(N,m);
ECM(N,m);
E:y^2=x^3+503660762927075472872361628044995212738882 95x+1, P=[0,1]
(19:57) gp > ECM(N,m);
E:y^2=x^3+1007555189787047542353899061065359630209096 27x+1, P=[0,1]
(19:57) gp > ECM(N,m);
E:y^2=x^3+552563176750580462713566349961174617473567964x+1, P=[0,1]
(19:57) gp > ECM(N,m);
E:y^2=x^3+397135561097002666990484115715239049553657671x+1, P=[0,1]
(19:57) gp > ECM(N,m);
E:y^2=x^3+759818664279760756844146034776484049491771197x+1, P=[0,1]
(19:57) gp > ECM(N,m);
E:y^2=x^3+764723571427193510106922997695099359109505002x+1, P=[0,1]
(19:57) gp > ECM(N,m);
E:y^2=x^3+796309481131631395974238268530964265887024821x+1, P=[0,1]
```

Μπορεί για τυχαίες επιλογές ελλειπτικών καμπύλων για $B = 20$ να βγάλει αποτέλεσμα,άρα η μέθοδος αποτυγχάνει. Θα δοκιμάσουμε με ένα μεγαλύτερο B

```
gp > B=10000;
gp > m=lcmfirst(B);
gp > ECM(N,m);
E:y^2=x^3+647180681144418184756772405769495273159223824x+1, P=[0,1]
gp > ECM(N,m);
E:y^2=x^3+665928129129180555125746328771005515697174511x+1, P=[0,1]
gp > ECM(N,m);
E:y^2=x^3+5434913917088165198424922409054262897611977O1x+1, P=[0,1]
  ***   impossible inverse modulo: Mod(2029256729,8006104706016552
  213927941800580881020534084 23).
```

Άρα το 2029256729 και το N έχουν μη τετριμμένο κοινό διαιρέτη. Το πρόβλημα έχει απλοποιηθεί σε ευκολότερο.

2.6 Το πρόβλημα του διακριτού λογαρίθμου σε ελλειπτικές καμπύλες

Ορισμός 20 *Έστω E ελλειπτική καμπύλη υπερ το $\mathbb{Z}_p$ και B σημείο της E. Το πρόβλημα του διακριτού λογαρίθμου στην E ως προς βάση B είναι το ακόλουθο.*

Δίνεται $p \in E$. Να βρεθεί n ακέραιος ώστε $nB = p$, αν τέτοιος υπάρχει.

Για παράδειγμα, έστω E ελλειπτική καμπύλη

$$y^2 = x^3 + x + 1 \text{ υπερ το } \mathbb{Z}_7.\ E(\mathbb{Z}_7) = \{0, (2,2), (0,1), (0,6), (2,5)\}$$

Αν $B = (2,2), P = (0,6)$ τότε $3B = P \Rightarrow n = 3$ η λύση στο πρόβλημα του διακριτού λογαρίθμου.

Το πρόβλημα του διακριτού λογαρίθμου σε ελλειπτική καμπύλη E είναι πολύ δύσκολο εκτός αν $E(\mathbb{Z}_p)$ είναι γινόμενο μικρών πρώτων ή η ελλειπτική καμπύλη είναι supersingular, δηλαδή $p|E(\mathbb{Z}_p)$.

2.7 El Gamal

Θα δούμε τώρα πως μπορούμε να ορίσουμε ένα public-key κρυπτοσύστημα κάνοντας χρήση ελλειπτικών καμπυλών.

Ξεκινάμε με ένα σταθερό, δημόσια γνωστό πρώτο p, και μια ελλειπτική καμπύλη E υπέρ το $\mathbb{Z}_p$, και ένα σημείο $B \in E(\mathbb{Z}_p)$.

Η Ανθή και ο Βίκτορας διαλέγουν αντίστοιχα κρυφούς τυχαίους ακέραιους m, n και υπολογίζουν και κοινοποιούν το mB και nB.

Για να στείλει ένα μήνυμα P στην Ανθή, ο Βίκτορας υπολογίζει ένα τυχαίο ακέραιο r και στέλνει το ζεύγος σημείων $(rB, P + r(mB))$

Για να διαβάσει το μήνυμα η Ανθή, πολλαπλασιάζει το rB με το μυστικό κλειδί του m και παίρνει

$$m(rB) = r(mb)$$

και το αφαιρεί από το δεύτερο σημείο

$$P = p + r(mB) - r(mB)$$

Για να σπάσει το κρυπτοσύστημα αυτό, θα πρέπει να λυθεί το πρόβλημα του διακριτού λογαρίθμου για τη E, το οποίο για κατάλληλες επιλογές της E είναι πολύ δύσκολο.

Η εταιρία Microsoft στην έκδοση 2 του Microsoft Digital Rights Management για τη δημόσια διανομή ψηφιακής μουσικής έκανε χρήση της ελλειπτικής καμπύλης

$$y^2 = x^3 + 3176890812513255034763174764138276932727469559 27x + 790528966078787587181205720257185354321006519 34.$$

ορισμένης στο σώμα $\mathbb{Z}_p$ όπου

$$p = 7859631023794288223766930248817149576126861574 29$$

Υπολογίζεται ότι

$$E(k) = 7859631023794288223766930248817149576126861574 29$$

και η $E(k)$ είναι κυκλική με γεννήτορα

$$B = (7715072162626498261706482685655798899077692541 76,$$

$$3901575102465566285252794592665149955625331966 55)$$

Όταν η Ανθή εγκαθηστά το πρόγραμμα προστασίας δικαιωμάτων στον υπολογιστή του, τότε δημιουργεί ένα ιδιωτικό κλειδί

$$n = 6708050311399105135175272076930604563002170544 73$$

το οποίο κρύβεται σε αρχεία του συστήματος (π.χ.blackbox.dll,v2hs.bla,IndivBox.key)

Για να κατεβάσει ένα αρχείο μουσικής, ο web browser της Ανθής, έρχεται σε επαφή με ένα Microsoft rights managment partner. Αφού η Ανθή δώσει το νούμερο της πιστωτικής της κάρτας μπορεί να κατεβάσει μια licence για να παίξει το αρχείο αλλά μόνο στον υπολογιστή της. Η Microsoft δημιουργεί την licence κάνοντας χρήση του El Gamal κρυπτοσυστήματος στην ομάδα $E(k)$.

Ένας άλλος χρήστης (αλλά και η Ανθή σε ένα άλλο υπολογιστή) δεν μπορεί να παίζει το μουσικό αρχείο αφού δεν γνωρίζει τον n.

Για την ιστορία της υπόθεσης ένας Hacher με το ψευδώνυμο «Beale screamer» έσπασε το σύστημα της Microsoft όχι κάνοντας επίθεση στο πρόβλημα του διακριτού λογαρίθμου, αλλά στην υλοποίηση της Microsoft. Το πρόβλημα που είχε να αντιμετωπίσει η Microsoft ήταν το εξής: πως είναι δυνατόν να αποθηκεύσει η Microsoft το secret key της Ανθής με τρόπο που η Ανθή να μήν μπορεί να το δει αλλά ο υπολογιστής της Ανθής να μπορεί; Αυτό είναι ένα αρκετά δύσκολο και ενδιαφέρον πρόβλημα, στο οποίο η Microsoft απέτυχε να δώσει ικανοποιητική λύση.

2.8 Γιατί να χρησιμοποιούμε ελλειπτικές καμπύλες;

Αν και οι υπάλληλοι της εταιρίας RSA Corporation μπορεί να διαφωνούν, υπάρχουν αρκετά πλεονεκτήματα στο να χρησιμοποιούμε την αμάδα μιας ελλειπτικής καμπύλης αντί της πολλαπλασιαστικής ομάδας $\mathbb{Z}_p^*$.

Τα ελλειπτικά κρυπτοσυστήματα με μικρότερο μήκος κλειδιού αποδεικνύεται να είναι τόσο ασφαλή όσο και το «κλασικά» $\mathbb{Z}_p$ κρύπτοσυστήματα με αρκετά μεγαλύτερο μήκος κλειδιού. Επίσης οι ελλειπτικές καμπύλες σαν τίτλος μεθόδου ακούγεται αρκετά όμορφα ώστε να προσελκύσουν το ενδιαφέρον καπιταλιστών χρηματοδωτών!

Κάποια κινητά τηλέφωνα χρησιμοποιούν κρυπτογραφικά συστήματα ελλειπτικών καμπύλων. Μήπως έχετε μια ελλειπτική καμπύλη αυτή τη στιγμή στην τσέπη σας;

Βιβλιογραφία

[1] Γιάννη Αντωνιάδη, *Ελλειπτικές καμπύλες, (Το θεώρημα του Mordell),* Ηράκλειο 1999

[2] *Algebraic Geometry and Arithmetic Curves.* Oxford Graduate texts in Mathematics

[3] Beauville, A. *Complex Algebraic Surfaces.* London Mathematical Society Student Texts, 34. Cambridge University Press, Cambridge, 1996.

[4] Silverman, Joseph H., *The Arithmetic of Elliptic Curves.* Graduate Texts in Mathematics, 106. Springer-Verlag, New York, 1995

[5] Lenstra, H. W., Jr. *Factoring integers with Elliptic Curves.* Ann. of Math. (2) 126 (1987), no. 3, 649–673.

[6] William A.Stein *Elementary Number Theory* Πρώτη έκδοση βιβλίου υπό συγγραφή. `http://modular.fas.harvard.edu/edu/Fall-2001/124/utm/`

[7] Silverman, Joseph H., Tate John *Rational Points on Elliptic Curves* Undergraduate Texts in Mathematics, Springer New York 1992.

[8] Jonh B.Fraleigh *Εισαγωγή στην Άλγεβρα*

[9] R.Chiurchill-J.Brown *Μιγαδικές συναρτήσεις*